



North American Association of Central Cancer Registries

NAACCR 2002 Workshop Report
Data Security and Confidentiality



February 5–7, 2002

**Aliso Creek Inn and Golf Course
Laguna Beach, CA**

Suggested Citation:

NAACCR. 2002 NAACCR Workshop Report: Data Security and Confidentiality. Springfield (IL): North American Association of Central Cancer Registries, May 2002. 56 pp.

North American Association of Central Cancer Registries 2002 NAACCR Workshop Report: Data Security and Confidentiality

**February 5–7, 2002
Aliso Creek Inn and Golf Course
Laguna Beach, CA**

Executive Summary

Lois Vogel, Workshop Co-Facilitator, welcomed participants to the North American Association of Central Cancer Registries (NAACCR) Data Security and Confidentiality Workshop and introduced the Workshop Planning Group. Dr. Holly L. Howe, NAACCR Executive Director, provided an overview of NAACCR and its role in supporting central cancer registries. She described NAACCR's five main goals: (1) maintain and establish standards for data collection, definition, and use; (2) provide education and training on those standards; (3) recognize standards that meet standards of high quality; (4) evaluate and publish cancer data from NAACCR members; and (5) promote the use of cancer registry data. Dr. Dennis Deapen, Chair of the NAACCR Data Use and Confidentiality Committee and Executive Director of the Cancer Surveillance Program of Los Angeles described the workshop goals and anticipated outcomes. The workshop was designed to initiate an effort that will result in a model and set of recommendations for operational confidentiality procedures as well as security and technology issues.

David Knapp, Chief Technology Officer of Knapp Communication Engineering, Inc. (KCE), discussed data and system security, monitoring, and auditing. KCE was hired as a security consultant and performed a security audit at the Cancer Surveillance Program of Orange County. Mr. Knapp's presentation included a detailed description of the International Organization for Standardization's model, translation services, routers and firewalls, challenges of system protection, monitoring and auditing, and costs and resources.

Dr. Thomas Taylor, Senior Statistician at the University of California, Irvine and Cancer Surveillance Program of Orange County and Dr. Deborah Bringman, Assistant Director of Registry Operations at the Cancer Surveillance Program of Orange County discussed lessons learned in pursuing Internet security for a central cancer registry. They detailed the steps taken by the registry in the development of a complete security system, including use of an outside consultant (KCE), purchase and installation of hardware/software, review of CERT guidelines, and the development of an *Employee Security Handbook* and a *Security Technical Manual*.

Steve Fuschlin, System Support Manager at the California Cancer Registry (CCR), presented on the development of CCR's cancer registry data system, Eureka. He described the circuitous route required to obtain help and information on the system design and requirements. Mr. Fuschlin addressed funding issues and described the key security and confidentiality elements of the Eureka system.

Andy Lake, Systems Analyst at Information Management Services, Inc. (IMS), described data security and confidentiality from a business perspective. IMS works closely with NAACCR, the National Cancer Institute, and the Surveillance, Epidemiology and End Results Program. He discussed provisions for receiving, processing, and releasing data; recommendations for maintaining confidentiality and a secure environment; and future challenges to data security and confidentiality.

Dr. Charles Key, Professor of Pathology and Medical Director of the New Mexico Tumor Registry at the Cancer Research and Treatment Center, University of New Mexico, discussed practical ways to safeguard confidentiality. He presented definitions of the terms privacy, confidentiality, and security. He also described the privacy, confidentiality, and security measures in place at the New Mexico Tumor Registry.

Ms. Wendy Nelson, Assistant Director of the Division of Health Policy and Systems Compliance (HPSC) at the Minnesota Department of Health (MDH), described HPSC's exemption allowing them to collect data on personal identifiers in the State of Minnesota, and opposition to this practice by privacy advocates. She described the HPSC/MDH experience, policies, and procedures in place at the HPSC and MDH, auditing, and next steps.

Dr. Howe distributed the Inventory of Best Practices Assurance of Confidentiality and Security to workshop participants. Participants made recommendations for minor revisions to the Inventory and suggested that the content and language of the Inventory be consistent with the content and language of the document to be produced as a result of this workshop.

Workshop participants met in two breakout groups, one focusing on registry operations issues, and one focusing on information technology issues. The breakout groups were provided with templates to help present their recommendations. In some cases, the templates were used—in other cases, breakout groups either modified the templates or developed an alternative format for presenting their recommendations. The registry operations group addressed three main issues: (1) physical security procedures for confidential data, (2) physical data security, and (3) electronic data security. The information technology group also addressed three main issues: (1) software and applications security, (2) network security, and (3) physical protection of hardware.

Data Use and Confidentiality Committee members met on the last day of the workshop. Products to be developed as a result of this workshop were discussed. A practical document will be developed that provides best practices and serves as a model for cancer registry IT security, confidentiality, and operations so that individual registries can specifically implement these policies and procedures and do not have to develop them on their own. A list of action items for the development of this document was created. Dr. Deapen and Ms. Vogel adjourned the workshop by thanking participants for their input and expertise.

Workshop Participants

(c) = Data Use and Confidentiality Committee Member; (s) = Speaker

Toshi Abe, M.S.W., C.T.R. (c)
Research Analyst
New Jersey State Cancer Registry
Cancer Epidemiology Services
New Jersey Department of Health and
Senior Services
P.O. Box 369
Trenton, NJ 08625-0369
(609) 588-3500
tabe@doh.state.nj.us

Deborah Bringman (s)
Assistant Director of Surveillance
Cancer Surveillance Program of Orange
County
University of California, Irvine
224 Irvine Hall
Irvine, CA 92697-7550
(949) 824-6856
dabringm@uci.edu

Dennis Deapen, Dr.P.H. (c)
Executive Director
University of Southern California School
of Medicine
Cancer Surveillance Program
of Los Angeles
1540 Alcazar Street, CHP 204
Los Angeles, CA 90033
(323) 442-2330
ddeapen@hsc.usc.edu

Eric Durbin (c)
Information Technology Manager
Kentucky Cancer Registry
2365 Harrodsburg Road, Suite A-230
Lexington, KY 40504-3381
(859) 219-0773
ericd@kcr.uky.edu

Thomas Faris, Esq.
Director of Regulatory Affairs and Quality
Assurance
IMPAC Medical Systems, Inc.
100 W. Evelyn Avenue
Mountain View, CA 94041
(650) 623-8807
tfaris@impac.com

Steve Fuschlin (s)
Information Technology Manager
California Cancer Registry
Cancer Surveillance Section
California Department of Health Services
1700 Tribute Road, Suite 100
Sacramento, CA 95815-4402
(916) 779-0290
steve@ccr.ca.gov

Susan T. Gershman, M.S., M.P.H., Ph.D.,
C.T.R.
Director
Massachusetts Cancer Registry
Department of Public Health
250 Washington Street, Sixth Floor
Boston, MA 02108-4619
(617) 624-5645
susan.gershman@state.ma.us

Barry A. Gordon, Ph.D. (c)
Director, C/Net Solutions
1936 University Avenue, Suite 112
Berkeley, CA 94704-1024
(510) 540-0778
barryg@asknet.org

Holly L. Howe, Ph.D. (s)
Executive Director
North American Association of Central
Cancer Registries
2121 W. White Oaks Drive, Suite C
Springfield, IL 62704
(217) 698-0800
hhowe@naaccr.org

Gary Hulett (c)
System Analyst
State Health Registry of Iowa
2205 Westlawn
Iowa City, IA 52242-1100
(319) 335-8609
ghulett@mail.public-health.uiowa.edu

Rachel Jean-Baptiste, M.P.H., Ph.D. (c)
Director of Science
North American Association of Central
Cancer Registries
2121 W. White Oaks Drive, Suite C
Springfield, IL 62704
(217) 698-0800
rjeanbap@naaccr.org

Charles Key, M.D., Ph.D. (s)
Medical Director
New Mexico Tumor Registry
University of New Mexico Cancer Center
2325 Camino De Salud, N.E.
Albuquerque, NM 87131-5306
(505) 272-5541
ckey@nmtr.unm.edu

Carol Kosary, M.A. (c)
Mathematical Statistician
Cancer Statistics Branch
Surveillance, Epidemiology and End Results
Program
National Cancer Institute
Executive Plaza North, Room 343E
6130 Executive Boulevard
Bethesda, MD 20892
(301) 402-5212
ck26s@nih.gov

David Knapp (s)
Chief Technology Officer
Knapp Communication Engineering, Inc.
14044 Lemoli Way
Hawthorne, CA 90250
(310) 644-5189
jacintha@verizon.net

Jacintha Knapp
President
Knapp Communications Engineering, Inc.
14044 Lemoli Way
Hawthorne, CA 90250
(310) 644-5189
jacintha@verizon.net

Andy Lake (c) (s)
Project Manager
Information Management Services, Inc.
12501 Prosperity Drive, Suite 200
Silver Spring, MD 20904
(301) 680-9700
lakea@ims.nci.nih.gov

Yang Mao, Ph.D.
Chief Environmental Risk Assessment
and Case Surveillance Division
Cancer Bureau
Health Canada
LCDC Building, Second Floor
Tunney's Pasture
All 0601C1
Ottawa, Ontario K1A 9L2
CANADA
(613) 957-1765
ymao@inet.hwc.ca

Mary L. McBride, M.Sc.
Epidemiologist, Cancer Control Research
British Columbia Cancer Registry/Agency
Cancer Control Research Unit
600 W. 10th Avenue
Vancouver, B.C. V5Z 4E6
CANADA
(604) 877-6122
mmcbride@bccancer.bc.ca

Stacey Neloms, M.P.H.
Director
Maryland Cancer Registry
Maryland Department of Health and Mental
Hygiene
201 W. Preston Street, Suite 300
Baltimore, MD 21201
(410) 767-5521
nelomss@dnhm.state.md.us

Wendy Nelson (s)
Assistant Director for Health Policy
and Systems Compliance
Minnesota Department of Health
P.O. Box 64975
St. Paul, MN 55164
(651) 282-3885
wendy.nelson@state.mn.us

Thomas H. Taylor, Ph.D. (s)
Senior Statistician
Cancer Surveillance Program of Orange
County
University of California, Irvine
224 Irvine Hall
Irvine, CA 92697-7550
(949) 824-7401
thtaylor@uci.edu

Lois Vogel
Facilitator
1 Gilson Drive
Rochester, IL 62563
(217) 524-6088
lvogelcomm@aol.com

Warren Williams, M.P.H. (c)
Health Scientist
National Center for Chronic Disease
Prevention and Health Promotion
Division of Cancer Prevention and Control
Centers for Disease Control Prevention
Koger Office Park
Davidson Building, Room 3246
2858 Woodcock Boulevard, Mail Stop K-53
Atlanta, GA 30341
wxw4@cdc.gov

Workshop Summary

Welcome and Introductions

Lois Vogel

Lois Vogel, Workshop Co-Facilitator and President of Lois Vogel Communications, opened the North American Association of Central Cancer Registries (NAACCR) Data Security and Confidentiality Workshop by welcoming participants. She introduced the Workshop Planning Group members, which included Dr. Dennis Deapen, Chair of the NAACCR Data Use and Confidentiality Committee and Executive Director of the Cancer Surveillance Program of Los Angeles; Dr. Holly L. Howe, NAACCR Executive Director; and Dr. Rachel Jean-Baptiste, NAACCR Director of Science; as well as Co-Facilitator Jacintha Knapp of Knapp Communication Engineering, Inc. (KCE), and herself.

Overview of NAACCR and Its Role in Supporting Central Cancer Registries

Dr. Holly L. Howe

Dr. Howe explained that NAACCR's mission is to serve population-based cancer registries throughout the United States and Canada. The organization has the following five goals:

- Maintain and establish standards for data collection, definition, and use.
- Provide education and training on those standards. As medical practice changes, rules for data collection and definitions must change; typically, they expand as more variables become important. NAACCR provides training on new standards and their implementation and operation in registries. NAACCR also is starting to provide training in areas of data use, research data, and past data quality.
- Recognize and certify registries that meet national, North American, and international standards of high quality. Registry data are evaluated on an annual basis, and registries are awarded certification status of either "Gold," "Silver," or "Other with feedback."
- Evaluate and publish cancer data from all NAACCR members in several formats, including a hardcopy monograph entitled *Cancer in North America*. The monograph, released every April, is a 5-year compendium of cancer incidence and mortality. This year, it will be a 3-volume monograph.
- Promote the use of cancer registry data in a variety of ways, including research and surveillance to reduce the burden of cancer in North America.

NAACCR activities, including this workshop, generally are driven by at least one of these five goals. Data confidentiality and security is another overarching priority for NAACCR. Maintaining patient confidentiality while collecting and using high-quality data presents

significant challenges. Dr. Howe discussed the need for confidentiality and ethics in collecting these data and balancing the right-to-privacy and the public's right to know. Each year, a plenary session at NAACCR's annual meeting is devoted to confidentiality and ethics—no other organization promotes confidentiality and ethics related to data collection and use to the degree that NAACCR does. She concluded her opening remarks by stating that workshops such as this where representatives from NAACCR, central cancer registries, government agencies, and private-sector organizations meet to tackle difficult issues will advance the whole community and discipline.

Workshop Goals and Anticipated Outcomes

Dr. Dennis Deapen

Dr. Deapen explained that a stereotype of cancer registries existed for many years, if not decades, where they were viewed solely as data gatherers and keepers. Although this stereotype may have been partly true, it has been rejected by most, if not all population-based cancer registries in the last decade or before because of NAACCR, forward-thinking cancer Registry Directors, and health department workers. A large amount of taxpayer dollars are used to collect these data, and they should be used to improve the public health. This presents a significant dilemma because registries want to use the data as maximally as possible, yet the data are highly confidential. Few things are held more privately by individuals today than their medical information, and yet, the American public clearly is supportive of cancer research and cancer control. When properly explained to them, the public understands the need for registries and for confidential data.

A major challenge is developing mechanisms to appropriately protect, secure, and release data while protecting patient confidentiality in a standard fashion so that each cancer registry does not have to develop them on their own. It would be inefficient to develop these processes and procedures on a state-by-state or region-by-region basis when the issues are overwhelmingly common across North America. In many registries, the technical aspects of data security exceed the capacity of registry staff. This can be due to the fact that registry employees traditionally have a medical records perspective and not an information technology (IT) perspective as well as for other reasons—in some cases, the IT department serving a registry is not under the registry's control but part of a larger institution. Dr. Deapen explained that the intention of the NAACCR Data Confidentiality Protection Workshop is to develop a model and set of recommendations for:

- **Operational confidentiality procedures**—what a registry staff needs to do in-house and in the field in terms of moving, examining, and editing the data; and all of a registry's activities up to the point of data release.
- **Security and technology issues**—this is a major challenge to cancer registries, and a model set of security policies are needed. It is important to note that a well-developed security policy may be, in and of itself, a highly confidential document. There needs to be a way to recommend a good security policy to cancer registries without divulging enough information that would help someone who wanted to hack into the system.

Data and System Security, Monitoring, and Auditing

David Knapp

David Knapp, Chief Technology Officer of KCE, discussed data system security, security monitoring and auditing, and costs and resources. KCE was hired as a security consultant and performed a security audit at the Cancer Surveillance Program of Orange County.

Data and System Security

Mr. Knapp explained that in secure communications, there is a firewall between the client and the server. There are three areas of communications that registry IT staff and Registry Directors should understand: (1) how computers communicate with each other, (2) the differences between routers and firewalls, and (3) networks. There are many standards in computer communications, and many companies with development teams generate standards intended to work across every platform that is part of that standard. Mr. Knapp described the International Organization for Standardization (IOS) Reference Model, which has the following seven layers: (1) Physical, (2) Data Link, (3) Network, (4) Transport, (5) Session, (6) Presentation, and (7) Application. The layers are divided into two specific regions:

- Application (the session, presentation, and application layers)
- Data Transport (the physical, data link, network, and transport layers).

Mr. Knapp explained that communications focus more on the Data Transport Region. He described the four layers in the Data Transport Region in detail.

Layer 1 (Physical Layer). This layer goes across the entire network and defines electrical and mechanical interfaces for media devices. It describes interface connections, levels, signal strength, and so on.

Layer 2 (Data Link Layer). This is the layer in which the different devices know how to communicate with each other. It defines media access control (MAC), which is analogous to telephones and telephone numbers. There also are media access/flow control protocols, which dictate how fast communication takes place. This includes 10Base-T and 100Base-T. Full duplex came out of 100Base-T, and registries should be on full duplex when working on these systems to avoid collisions, or “bad packets,” which can cause a program to malfunction. The devices that work in Layer 2 are bridges and switches. Switches are actually bridges, only faster. Bridges are all hardware based; there is no software involved. Mr. Knapp presented a diagram illustrating client-server communication across a Layer 2 device.

Layer 3 (Network Layer). Communication on the Internet is tunneled through transmission control protocol/Internet protocol (TCP/IP). The components of TCP/IP are an address, subnet mask, default gateway, minimum transmission unit, and frame layout. The devices involved in Layer 3 communications are routers, Layer 3 switches, and firewalls. Mr. Knapp noted all three of these devices basically carry out the same function. Firewalls started out as applications on hosts, but because operating systems are general, firewalls should be run on dedicated, specialized hardware whose only function is to run the firewall.

Layer 4 (Transport Layer). Mr. Knapp described port assignments. In Layer 4 communications, the port number and the protocol must be known. Different vendors use different protocols. He explained that there are applications that require both a UDP port and a TCP port to be open, and cautioned against opening a user datagram protocol (UDP) port where a TCP port should be open, because this can cause applications to fail. In the early days of computer development, each port number was assigned to an application. Applications were set on these ports, so that the host could understand when a packet came in, it could look at the port number and determine who is running that application, and send it up. More recently, other types of ports have been utilized known as remote procedure ports (RPCs). With these ports, it is not the network or the transport layer that decides what the application is; it is a much higher layer in the Application Region. RPCs are dangerous to open to the Internet because an outside individual could gain access to and use computers on the network.

Mr. Knapp described the two basic translation services: (1) address resolution protocol (ARP), and domain name service (DNS). ARP converts MAC addresses in Layer 2 to IP addresses in Layer 3. DNS converts IP addresses in Layer 3 to system names in Layer 7. He described the functions of routers and firewalls. Routers allow communications by default, which is why routers should not be used as firewalls. Routers have a stateless connection base—they do not handle the control between the client and the server. Mr. Knapp explained that routers do not control sections; they just push data through, which is why they are so fast. Both routers and firewalls perform network address translation, which basically hides private addresses. It also allows a number of people at the same address to communicate if there is a device that does network address translation to the Internet or within the company. Port address translation is similar, but it uses one IP address and can have hundreds of clients behind it. Mr. Knapp advised participants to avoid port address translation because it can change fixed port numbers in certain applications.

Before firewalls were introduced, routers had a stateless control and were essentially access control lists. Access control lists help routers by stopping communication. Everyone who connects to the Internet should have an access control list on their router to prevent private IP addresses coming in from the Internet as a security measure. The access list also should not allow the IP addresses that make up the registry's network to come in from the Internet, because a hacker can fake their source IP address—that is how denial of service attacks work. Access lists also prevent a hacker from using a registry's machine in an attack outside of a registry's organization.

More recently, routers started introducing firewall software, an intrusion detection system that allows for stateful connections to ward off attacks. Firewalls can perform routing and bridging functions similarly to routers. Firewalls have stateless connections and access control lists, but are limited by the number of connections. Firewall vendors are able to sell their products to both small and large companies because they license the number of connections that go through. This is why firewalls vary in price. Cancer registries probably should invest in the more expensive firewalls because large numbers of people will be coming onto their networks. Each attack takes a connection. The more connections on a network, the less likely it is to go down under an attack. Mr. Knapp briefly described all of the components of a network, including IP address

space, name service, wide area network (WAN) service (public and private), routers and firewalls, switch/hub, cable, and hosts providing applications and data.

Mr. Knapp described the challenges of system protection in terms of the following six design steps:

Identify the threat. Mr. Knapp recommended starting with a machine that has no connections and then giving it the types of transmissions that it needs to communicate with clients. Each time another component is added, the system's security is decreased to some degree. To track this, he recommended that registries pose a series of questions. What access is required? To have a secure server and secure data communicate with other users, there will need to be a local area network (LAN) as well as possibly a modem and/or cluster connections. What is required to maintain and operate the system? In developing a network, remember to ensure that developers have access to the system, the system can communicate with its backup system, and that system administrators may want remote access to the system to support the hardware. Who will be working with the data? Each person and machine added weakens security. Mr. Knapp recommended adding another interface to the firewall and keeping all the support individuals on that subnet to allow users of those specific machines to perform their functions without jeopardizing the firewall's security. What is required to go through the firewall? Ask this question every time the design process is changed. Who will be sending and receiving data? If these individuals are known, then appropriate questions regarding IP addresses, secure sockets, and encryption tools can be asked. Mr. Knapp noted anything not covered by these questions is a threat that must be protected against.

Identify the level of access. After identifying users of the system, their access must be identified, which can be done via protocol, IP address, user account, and so on. Mr. Knapp noted that user account should be the last level of security. Never make general user accounts, and strip the general passwords for general users off the system, because they are turned on by default. The same principles apply to firewalls and routers. Any kind of equipment on a network is a security risk, and if it is not controlled by the registry, it could be controlled by someone from outside the registry. Address how the firewall will support access, and be aware that the more a firewall is opened, the more it allows communications and becomes a router. Test the firewall to ensure that it prevents unauthorized access.

Develop a security policy. Individuals who are responsible for developing security policies at registries should explain what they want in lay terms and then give it to an IT specialist who understands access lists and firewalls. Avoid having multiple holes in a system by having each system isolated behind a firewall on its own port and translated so that if someone gets into a system, they cannot do anything with it. If a network has multiple systems open, a hacker could exploit that vulnerability and use those other holes to gain access to data or use the network's equipment in an attack. If the type of access is limited by protocol and port and a hacker is able to exploit it, chances are they cannot do anything else to any other server. The ideal is to have a dedicated system for each function. If users require Web access into a registry's system, only one of the registry's systems needs to have Web access open. If these systems are separated on different subnets or networks, it is much easier to control access to them.

Identify the availability. Everyone wants 99.99 percent availability, which is hard to achieve, particularly with the Internet that can go down periodically. Registries need to have backup systems. Redundancy dictates design difficulty because of broadband costs. There probably will be an Ethernet handoff across fiber or copper, and getting that kind of connection between two facilities can be very expensive, especially if it is not on private property. Connecting two buildings together to have redundant systems across LANs is very expensive. Keep in mind that the more complicated the system and its backup, the more senior-level staff are required to troubleshoot and fix it. The higher the bandwidth a registry has to the Internet, the more it is able to sustain an attack and keep its availability up. The best way to prevent denial of service attacks is to outbandwidth hackers, because they need multiple machines to work together to take the registry's network down. Mr. Knapp explained that if a registry has more bandwidth than the hacker can offer, then it will not go down, and the hacker can be blocked with the registry's firewall. Also, it is important for registries to ensure that their hardware's capabilities are larger than the registry's access to the Internet. This will allow the registry's firewall to filter more and will prevent it from going down and having problems.

Develop, Design, and Implement. Beware the four-tier system. In this system, projects are theorized by management, designed by networking, and implemented by consultants, but the registry is left on its own, with no idea of what is going on. A more effective approach is the five-phase project, which progresses through discovery, design, procurement, implementation, and operation.

Best practice design. Mr. Knapp advised that registries try to put as many layers as possible between their systems, but cautioned that if a network has the same hole through each layer, it defeats the purpose of having layers. Data and machines have to be able to pass through these layers, but the system should be limited as much as possible to only that which is needed to get the job done. When buying equipment, Mr. Knapp recommended using companies that have demonstrated experience and reliability, and purchasing equipment that is widely used. He also discussed the importance of a 24-hour monitoring service. The system should do its job during the workday, and protect itself at night, when hackers are more active, and it needs to be monitored for attacks. Each registry should establish a security policy and change control committee. In a security policy change control committee, a number of individuals make decisions on security policy changes as a team, rather than just one or two individuals. A design may look good on paper, but once the construction and maintenance of the system take place, things can go wrong and changes are going to be made. It is critical to ensure that changes are implemented with the same design criteria and security policy. Registries should refer to security standards that are available from various vendor, government, and particularly, independent groups (e.g., System Administration, Networking and Security [SANS]; CERT Coordination Center [CERT]; and National Information Protection Center [NIPC]).

Mr. Knapp also described the challenges of system protection in terms of the following three implementation steps:

Verify that design criteria are met. Review the overall design against the security policy. Ensure that if changes are made to the system, the system is taken off the network, the security policy and change control committee has met, and everyone is in agreement that the change is

acceptable. Have a representative from every team get involved to sign off on final configuration. Do not make changes on a Friday; the best time to make changes is early Monday morning, when staff are available onsite to meet and troubleshoot.

Verify that the audit is working. The final task when a network is constructed is to ensure that there is a way to prove that it is working. This can be accomplished via a reproducible audit, which can be run through a software package or through an outside company. Always look for a way to audit the system and do so frequently. Audits should be run after every change to the system. Mr. Knapp again advised against making changes to the system on Fridays. He reminded participants that developing a security plan and implementing and maintaining the plan are ongoing processes.

Create a change control process. Every time a change to the firewall or security system is proposed, ask the following question: “Are these proposed changes going to maintain or enhance the primary objective of the firewall?” If the answer is yes, then have a development system that allows for verifying that the change is working and that it maintains or enhances the primary objective of the firewall. If the answer is no, then the change will degrade the firewall, and serious consideration should be given to whether the change is absolutely necessary. Do not rush into or be pressured to make changes, which is how security systems often break down.

Network Security Monitoring and Auditing

Make sure that someone is monitoring the system and is being notified if anything goes wrong. Mr. Knapp advised the following:

- All access should be monitored—if the system has a firewall with a security policy built in, there should be another machine that knows the security policy and checks every packet and every connection to authorize them.
- All host activity should be evaluated to see if there are any compromises in security.
- All system maintenance/changes should be recorded.
- License connection activity should be recorded.
- Firewall, central processing unit, and memory status should be monitored.
- Application server syslogs should be monitored.

A third-party service can be used to conduct security audits on a registry’s network. This service should test regularly with a proven technique, and test after every change—never make a change without testing it to make sure the change is in place. Also, be aware that changes can trigger bugs. Above all, Mr. Knapp said, do not become complacent, because hackers work every day. He recommended joining security network groups such as the Information Systems Security Association (ISSA), CERT, SANS, and NIPC.

Mr. Knapp presented KCE’s vision of security. During the years of early Internet development when universities were connected for grant research purposes, there was essentially no security; it was a very “trusting” network with good intentions. At present, e-commerce, government, private institutions, the military, and everyone else want to be connected—all of these are targets for hackers. Technologies such as firewalls, intrusion detection systems (IDS), routers, access

control lists, and virtual private networks (VPNs) have been developed. In the future, the same targets will exist with the addition of home networks as DSL and cable modems increase high speed Internet use from homes. Mr. Knapp predicted that home network security will become a significant challenge in the future. More highly specialized security technology will be developed to address these issues.

Mr. Knapp also described KCE's monitoring service, which performs all of the tasks described in his presentation—one of the few companies that does so. KCE has applications that look for signatures with the advantage of being able to house the same security policy that their clients' systems run on and audit everything that is happening. Applications only look for signatures, while KCE's service looks for both signatures as well as patterns. KCE's equipment is housed onsite in a locked box and resides on the back side of the client's firewall. KCE allows local Web access to their equipment to pull records from the security equipment, store them back on the database through a dedicated private line, and provides a Web interface to pull those records back. This provides a high-level overview of things that are critical to the client's system.

Costs and Resources

System design and implementation can be done in-house or by utilizing a third party. Mr. Knapp recommended that registries partner with other organizations that have expertise and experience in designing and implementing security systems. He stressed that this is an ongoing process, and that once a security system is in place, it takes a constant effort to ensure that it works properly and is kept up-to-date. As much as possible, budget for the high end—security consultants are expensive (up to \$250 per hour), and they tend to want to work after hours and on weekends because that is when the system is on downtime (and when the consultant's fees are even higher). Other options are using purchase orders, fixed contracts, or utilizing full-time staff with the appropriate expertise and experience. It is critical to have an ongoing, long-term relationship with the individuals or company that is designing, implementing, and monitoring the security network.

In terms of equipment, Mr. Knapp suggested using a reputable firewall/IDS company and again, budgeting for the high end. Do not invest in a less expensive system that has the potential to become overrun and pose a security risk. He estimated that a low-end figure is approximately \$40,000, and a high-end figure is roughly \$200,000. Avoid hosts with software on it as the firewall, and select hardened operating systems for platforms. Although some operating systems can be obtained via the Internet at no cost, hardware is needed to run them. Low-end hardware costs about \$25,000, and high-end hardware about \$100,000.

With regards to maintenance, be aware that as part of the manufacturer's warranty, onsite service is available to replace and troubleshoot hardware. However, some maintenance plans provide inadequate support, and even reputable companies may hire ineffective employees or other companies to carry out the service contracts. Always watch the person who is doing the service work or have someone qualified to watch that person. Mr. Knapp noted that companies exist that will conduct in-house auditing and monitoring for an annual fee.

Discussion

When asked what secure data transfer standards are relevant to cancer registries and NAACCR, Mr. Knapp responded that VPN and data encryption currently are widely accepted security standards for the transfer of sensitive data. VPNs are used more often. Encryption modules, in which two different pieces of equipment use different types of codes and know each other by that hardware, are newer. If there is a network or subnet communicating secure data with another network or subnet, encryption modules are a viable, but expensive option. Secure socket or open encryption systems are additional options.

Although Mr. Knapp recommended 24-hour system monitoring, most cancer registries are not 24-hour operations. He suggested having IT staff at the registry unplug the system or disable the appropriate port at the end of the day, after the backup process has occurred, to prevent intrusions. In terms of auditing, there are nationwide consulting services that can test registry systems in-house or remotely. References for these companies may be available through organizations such as CERT and SANS. These organizations also are a good resource for information on what to look for when hiring IT staff. Mr. Knapp closed his presentation by noting that security system designs need to have built-in policies and plans for addressing system intrusions. CERT provides a great deal of relevant information on this topic as well as a list of procedures to follow in the event of an intrusion.

Lessons Learned in Pursuing Internet Security for a Central Cancer Registry *Drs. Thomas Taylor and Deborah Bringman*

Dr. Taylor, Senior Statistician at the University of California, Irvine and Cancer Surveillance Program of Orange County, explained that security matters affect many aspects of registry operation. Many of these are well understood, such as employee confidentiality agreements; background checks for new hires; locks and keys; policies on shredding, mailing, and e-mailing; and disaster recovery. However, there are aspects of registry operation security that are unknown. These can be divided into “known unknowns,” or questions that a registry knows that it needs to answer (e.g., how to choose a firewall, who will monitor it, who will set it up, what are the steps to take if it is not functioning properly), and “unknown unknowns,” which can be much more dangerous. The Cancer Surveillance Program of Orange County needed outside help to address both types of unknowns.

Dr. Taylor emphasized the importance of making a blueprint security plan—this is a tedious effort, but it is important to document what has been done, what the problems are, and the responses to problems. CERT, which has standards recognized by the federal government, provides an excellent framework within which to do this. Dr. Taylor and colleagues at the Cancer Surveillance Program of Orange County undertook measures to make the registry CERT-compliant. The appearance of security is important for convincing the public, third parties, and site visitors. Being CERT-compliant not only provides security, but also it provides the appearance of security.

The registry used an outline from CERT as a starting point in developing a security policy. When they needed help with designing a system with a firewall to protect their server, they found that the University's IT staff did not have the appropriate experience—their department is the only one on campus that has medically privileged data. After meeting with vendors to design a system, they bought what was thought to be the appropriate hardware. However, a large proportion of this initial investment was lost because the designer was no longer with the vendor who helped design the system, and the designer left no clear instructions on how to install the hardware. With the help of an outside consultant (KCE), however, they now have a cutting-edge security system.

Dr. Taylor provided the following recommendations for registries when screening consultants: (1) look for excellent references and ask the registry's Internet service provider for recommendations; (2) avoid consultants tied to specific brands; (3) avoid consultants who offer "plug-and-play" solutions; and (4) find a consultant who is willing to commit long-term—they have to help to review the firewall logs and system logs, train registry staff, help respond to attempted breaches, and maintain the defense as technology evolves. It is important to have a security plan with an active practice. Dr. Taylor also suggested avoiding consultants who have small retainers but large hourly charges for onsite support.

The tighter the security system, the less convenient it is for people to break in. It is pointless to have a system and then start letting people back in again, so stick to the policies in your security plan. Think carefully about having an independent outside auditor come in and test the system. What vulnerabilities are created during their testing? Are vulnerabilities removed when the testing is complete? Registries can conduct self-monitoring to a degree—the wired world is constantly testing registries' Web sites and if registry IT staff monitor the logs, they can obtain "test results" right away. Dr. Taylor closed his remarks by reminding participants that an Internet security plan is not a "set it and forget it" effort, it is a consistent process.

Dr. Bringman, Assistant Director of Registry Operations at the Cancer Surveillance Program of Orange County, described the steps taken to improve the security of their computer systems. In working with KCE, the registry developed a network architecture and firewall as well as a security manual that includes policies and procedures to prevent network computer systems against security compromises. The registry decided to use CERT security practices as a guide to formalize their security policies. CERT is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center at Carnegie Mellon University. CERT strives to increase awareness of security issues and help organizations improve the security of their computer systems.

CERT's Web Site (www.cert.org) includes a great deal of information, including seven Security Improvement Modules that address the important but narrowly defined problem of network security. These modules are:

- Security for Information Technology Service Contracts
- Securing Desktop Workstations
- Responding to Intrusions
- Securing Network Servers

- Deploying Firewalls
- Securing Public Web Servers
- Detecting Signs of Intrusion.

Dr. Bringman noted that CERT links each module to a series of Practices and Implementations. The Practices section describes choices and issues to be addressed in solving network security problems and makes recommendations. The Implementation section describes the necessary tasks to implement the recommendations. CERT groups the Practices into general steps, including:

- Harden and secure your systems by establishing secure configurations
- Prepare for intrusions by getting ready for detection and response
- Detect intrusions quickly
- Respond to intrusions to minimize damage
- Improve your security to help protect against future attacks.

Dr. Bringman described the CERT best practices for securing desktop workstations and networks. CERT provides instructions on how to configure computers for user authentication. It also provides information on configuring a system to use hardware-based access control if available, remove unneeded default accounts or groups, check password policy and set account passwords accordingly, ensure that users adhere to password policies, require reauthenticity after idle periods, deny login after a small number of failed attempts, and other authentication mechanisms as required. Policy considerations should document and describe under what conditions an account is created or deleted, require appropriate authentication of all users, include an appropriate password policy, and require users to shut down and lock their workstations at the end of the day.

She and her colleagues reviewed relevant CERT best practices, determined how they could be applied to the registry, and developed their security policy and procedures. Based on these efforts, they developed two manuals: (1) a *Security Technical Manual* that is confidential and detailed enough so that if something should happen to their IT staff, the registry could hire an IT expert who could refer to it and quickly learn the system; and (2) an *Employee Security Handbook* that informs employees of the registry's security measures. All employees must read the *Handbook* and sign a confidentiality agreement. The *Handbook* also is available in electronic form for employees to read and refer to. Dr. Bringman noted that both policy manuals have the following major sections: (1) network security, (2) Web security, (3) database security, (4) physical security, and (5) disaster recovery. She concluded by stating that developing security policies and procedures is an exhausting, never-ending task, and that these efforts are wasted if the policies and procedures are not strictly enforced.

Development of the California Cancer Registry Data System

Steve Fuschlin

Mr. Fuschlin, System Support Manager at the California Cancer Registry (CCR), has been overseeing the construction and implementation of CCR's statewide data system, Eureka. He described efforts to obtain help with standards to build this system from California's Department of Information Technology, the Department of Health Services (DHS) Information Technology Services Division, and the DHS Office of Automation Systems and Internet Services. None of these resources were able to provide guidance—he noted that the State of California is 10–20 years behind the technology curve. Mr. Fuschlin also described how attempts to obtain help from a major cancer center that was implementing a new cancer registry system were unsuccessful because the center did not want to share its information. He then contacted the cancer center's contractor, who was unable to provide information about that specific system, but was able to help him gain an understanding of the technology and the minimum set of requirements for the system. To ensure that the technology was appropriate and that best practices were being followed, Mr. Fuschlin gathered information from vendors such as Pacific Bell, Cisco, Symantec, and Microsoft; industry-wide consultants such as Gartner Group and Meta Group; local consultants; conferences; and the Health Insurance Portability and Accountability Act (HIPAA).

Mr. Fuschlin conducted a best practices exercise with other companies nationwide, comparing the standards between banks, insurance companies, airlines, and a hospital. Surprisingly, Kaiser, which was expected at the beginning of the exercise to have best standards because they use health-related medical information, was furthest behind in their standards. Banks on the other hand were 10 years ahead of most of the other companies, while hospitals were 10 years behind. To prevent efforts that “reinvent the wheel,” he suggested that registries examine the standards and policies in place at organizations such as banks to determine best practices. Specific solutions for implementing best practices may be found through vendors, consultants, and HIPAA.

Mr. Fuschlin and the CCR found affordable security solutions using an approach that examined the overall cost of security and realizing that security “affordability” involves more than money—there are tradeoffs between security and other business needs. He recommended that registries keep in mind the larger issue of affordability versus the cost of a router or firewall. His approach with the CCR was to provide management with as much data as possible to let them make a good business decision. He provided three options, in order from most expensive to least expensive:

- Solution X (most secure)
- Solution Y (passes the test of “due diligence” and/or meets industry standards)
- Solution Z (does not meet industry standards, presents the risk of lawsuits).

There are ways for registries to save money so that they can purchase better equipment, but Registry Directors and those who purchase the equipment must be willing to educate themselves. This is no longer only the IT person's domain, it also is the management team's responsibility to become educated so they can help to make informed decisions. Online conferences and

presentations by vendors are examples of educational opportunities that cost very little. Other examples include use of Internet IT professional chat rooms and free, state-sponsored training that is available in some states. He advised registry staff to always negotiate and ask for donations when purchasing equipment. Specifically, always negotiate the government rate down. As an organization, cancer registries should band together so that they approach vendors or consultants; they are bargaining from a group position rather than an individual position.

Mr. Fuschlin described the key security and confidentiality elements of a system like Eureka or other central cancer registry data system. There are four key elements: (1) physical security, (2) application security, (3) network security, and (4) business process. He noted that many registries overlook the business process element. The Eureka system is being built so that access is controlled internally, allowing only the appropriate individuals to access the data depending on their job. Users are assigned with either dependant or independent capabilities. Users with dependant capabilities must be associated with a specific reporting source or region. Those with independent capabilities can perform functions at any reporting source/region. For example, if a user has a dependant capability associated with a hospital, their access is restricted to the hospital's data. If an individual has independent capabilities at the regional level, they may perform tasks for any hospital within their region. Users can be assigned multiple roles and have capabilities added to their functions.

On the application side, every change is logged and audited. Internally, there will be a firewall, a Web server, and then another firewall. The data will reside behind the second firewall. Mr. Fuschlin noted that this is a California Department of Information Technology-approved system. In terms of the actual transmission of the data, he explored a VPN solution, but it was found to be too difficult because of work station identification authentication issues at hospitals. Therefore, he is considering a secure socket system (128-bit encryption), or a point-to-point connection. Mr. Fuschlin expressed the hope that data security and confidentiality become more of a business issue, and that business processes get built around them, rather than just assigning one person to handle all of these issues. He noted that building, implementing, and maintaining a secure data system is not a one-time solution because the technology is changing so rapidly. It is a business process, and that is what needs to be developed.

Data Security and Confidentiality From a Business Perspective

Andy Lake

Andy Lake, Systems Analyst at Information Management Services, Inc. (IMS), works closely with NAACCR data and is responsible for coordinating the statistics NAACCR generates for publication and for registry certification. IMS works closely with the National Institutes of Health (NIH) and National Cancer Institute (NCI) on data processing and IT issues. The company also works with the Surveillance, Epidemiology and End Results (SEER) Program by receiving SEER data and running edit checks. Mr. Lake described the constant balancing act facing IT administrators who must make the level of data security acceptable without making it too cumbersome to access and use the data. When security measures are sacrificed to make it easier for the intended people to access the data, it unfortunately also makes it easier for unwanted individuals to access the data.

Provisions for Receiving, Processing, and Releasing Data

Mr. Lake described some of the general confidentiality practices used at IMS. New employees at IMS are first asked to sign a confidentiality agreement stating that they will not misuse or inappropriately release the data. Employees are assigned a user identification that allows them to access to the IMS network and are instructed to create a password that includes both alpha and numeric characters in it. These steps and others are explained in detail in IMS' employee handbook. After an employee has a password, access to appropriate files on the IMS network are assigned by IMS' IT Administrator. All files on the IMS network have specific permissions assigned to them, and the IT Administrator has control over their read and write privileges. IMS' network system is in a locked room with access limited to only a few select IT employees and administrators. The system performs routine backups on a daily and monthly basis. In addition, backups of the system are stored off the network. The system has the capability of producing an audit trail to provide information on who has used files. Audits of IMS' system are performed on a routine basis.

Within the last 2 years, IMS has implemented a data encryption system. All data received from NAACCR's Call for Data are encrypted and transmitted via file transfer protocol (FTP). After they are downloaded from the FTP site, the data are stored on a secure data directory with access limited to only those working on the NAACCR project. Only read-access is given to those files. IMS handles patient questionnaires in its dealings with the NIH and clinical trials. These papers are kept in a secure file in a locked room with limited access. Hardcopies of data are shredded whenever they are disposed. IMS controls data release very tightly. All requests for data must come in writing from the NCI or NAACCR. Mr. Lake noted that because IMS is a contractor, Freedom of Information Act (FOIA) requests do not apply. All FOIA requests must be processed through the NCI, NAACCR, or the Centers for Disease Control and Prevention (CDC).

Recommendations for Maintaining Confidentiality and Secure Environment

Mr. Lake gathered recommendations from IMS' IT staff for developing and maintaining a secure confidential environment. Registry staff must understand that this is a very serious and complex undertaking that requires a great deal of up-front work. Start with a basic plan, which is difficult to put together, and build in the necessary detail. Registries need to have robust security systems that have many layers. At IMS, there are many security systems with the idea that not one system is going to offer full protection, but the many levels together create a strong environment and offer better protection. The risk of lower data security must be weighed against accessibility to the data. Clients need to access the data, and registries should ask themselves how much security they are willing to give up to provide that access? Registries also should develop a good disaster prevention and recovery plan.

Future Challenges to Data Security and Confidentiality

Personnel will always be an unknown factor. Any registry could hire a person and ask them to sign confidentiality agreements, but despite this, that individual may misuse or give away data or sabotage the registry's system. In addition, human errors do occur. A major challenge is finding skilled, experienced individuals in the IT field who are familiar with the security needs of cancer registries. Cancer registries should keep up with changes in security standards.

Some Practical Ways To Safeguard Confidentiality

Dr. Charles Key

Dr. Key, a Professor of Pathology and Medical Director of the New Mexico Tumor Registry at the Cancer Research and Treatment Center, University of New Mexico, described a 1998 National Research Council (NRC) publication titled *For the Record: Protecting Electronic Health Information*. This document provided simple and useful definitions for terms such as privacy, confidentiality, and security. Although limited, these definitions are useful. Dr. Key presented NRC's definitions of these terms:

- **Privacy**—An individual's desire to limit the disclosure of personal information.
- **Confidentiality**—A condition in which private information is shared or released in a controlled manner.
- **Security**—A number of measures that organizations implement to protect information and systems.

Dr. Key noted that the definition of security includes efforts to maintain confidentiality as well as to ensure the integrity and availability of that information and the information systems used to access it. The data as well as the integrity of the system need to be preserved and protected.

Safeguarding confidentiality requires: (1) a well-planned facility, (2) limited access, (3) secure files, (4) protected computers, (5) controlled output, (6) documented procedures, (7) a respected Director, (8) dedicated staff, and (9) responsibility and commitment. In 1998, the University of New Mexico constructed a new building, and the New Mexico Tumor Registry moved into the ground floor. The new building gave the registry the unique opportunity to provide some degree of input into how the new building was laid out.

Access to the entire first floor of the new building is controlled by card swipe. This keeps the facility secure and has significantly decreased unnecessary traffic in the building. There is a security employee/building manager whose desk is in the main foyer area. Additional security to this building has been put in place because there is a biosafety level three laboratory on the top floor. Visitors enter the foyer of the building, sign in with the security person, and are given a badge. Once they pass through the door to the registry, they are met in a reception area and escorted throughout the registry. The area of the registry where the patient records and laptops

are stored requires additional access that is tracked. Many of the registry's abstractors travel large distances across the state. The registry recommends that these employees store their laptop in the trunk of their car while traveling.

Workstations within the registry office have screensavers and passwords. Work areas are kept devoid of patient material when the employee is not present and using the material. At the end of the day, records are not stuffed in drawers or cabinets, but are returned to the file room. The main computer room requires both card access as well as a key. Master files with patient identifiers are stored on a separate computer from that which contains the analytic files that the biostatisticians and researchers access. The chart room where the paper is filed includes movable shelves, which is an efficient way to store the data. This room is always locked, and any time the room is entered, it is recorded. Inside the chart room there is space for review of the records. Any paper that contains personal information that is not destined for the file is shredded. Since 1998, the registry has revised its policies and procedures twice.

Dr. Key noted that it is an ongoing effort to incorporate new ideas and new recommendations into their policy and procedure manual as well as their training procedures. The registry continues to work on protecting computers and controlling the output of printed material from registry operations. All of this requires not only the procedures and documentation of the policies, but also a respected Director who has the authority to ensure that the rules are enforced. All of these technical innovations do not work without a dedicated staff who have a culture of responsibility and commitment to the maintenance of individual privacy and confidentiality and security of the data.

Discussion

Dr. Key explained that records can leave the chart room and enter the secured workspaces if records need to be combined. The folders housed in the chart room may include pathology reports and death certificates. The registry recently implemented a system in which electronic records can have scanned images of documents such as pathology reports or death certificates appended to them. All paper records are returned to the chart room at the end of the day. The registry currently scans new data from paper records, which gradually will decrease the amount of paper records at the registry. The registry has controls in place for who can amend or append information in an existing file.

Dr. Key explained that most of the work with the registry's database includes analytic files that do not contain individual identifiers. The registry receives very few requests that require pulling a chart and looking for specific information in that chart. The New Mexico Tumor Registry's level of security is more rigorous than that of most cancer registries, and its employees understand and cooperate with its policies and procedures. Dr. Key noted that cancer registries should be at least as secure as the medical records department of a hospital.

Protection of Confidentiality Initiative

Wendy Nelson

Ms. Nelson, Assistant Director of the Division of Health Policy and Systems Compliance (HPSC) in the Minnesota Department of Public Health (MDH), works with encounter-level data—claims and enrollment data from health plans. As part of the HPSC Encounter Project, she began collecting claims and enrollment data from health plans in 1995 to monitor and improve the effectiveness of health care in Minnesota and to answer the question of whether these data can be used for this type of research. As part of the project, data on personal identifiers and medical procedures are collected, which is a cause for concern among some vocal groups in Minnesota.

The HPSC/MDH Experience

The State of Minnesota has one of the toughest medical records access laws in the Nation. Investigators cannot obtain medical records to conduct research in the State of Minnesota without individual consent. However, the HPSC has an exemption and statutory authority to collect these data, which bothers some individuals and organizations—such as the Minnesota Citizens Council on Healthcare, which does not want cancer registries or immunization registries to exist in the state. The HPSC is required to encrypt the personal identifiers, and the data can be released only in a form that makes it “impossible” to identify individual patients—meaning they cannot be released at all.

Privacy advocates from the Minnesota Citizens Council on Health Care have enrolled Minnesota’s Attorney General, who is running for Governor and believes that the HPSC should not be allowed to collect the data. The media also has taken the group’s side. A bill was introduced in 2000 to take away the HPSC’s exemption. The bill was not passed and served as a wake-up call to Ms. Nelson and colleagues, who recognized that they not only needed to implement the security requirements mandated by legislators, but also had to have, from a public relations standpoint, an extremely high level of security above and beyond the actual requirements. They also realized that they had to justify the use of the data and withstand any level of inspection. The HPSC has extensive data and network protections, including routers, firewalls, separated databases, an applications server, a data server, and so on. They encrypt data being transferred, and replace or encrypt identifiers. Ms. Nelson explained that only three people have access to the entire database. Individuals who want to access the database must provide justification for doing so and are only allowed to access what they need. Ms. Nelson and colleagues use a bank safe deposit box to store backup tapes.

HPSC Policies and Procedures

To respond to privacy advocates in Minnesota, the HPSC needs to demonstrate that it cares deeply about the privacy and confidentiality of health care data. The Division has developed extensive policies and procedures to accomplish this. The HPSC trains staff on security and data practice responsibilities. An audit was conducted at the department and division levels. The HPSC defined user responsibilities, described its security policy, and defined how people should

create their passwords—using two numeric and at least one alpha character. Passwords have been developed for the network, database, and screensavers. A shredder is used to destroy all nonpublic data. In terms of hardware security, policies are in place that address laptop security and ensure that employees turn off their computers at night. The HPSC does not allow use of PC Anywhere software; a more controlled, secure method of remote access is used. Employees are forbidden from saving nonpublic data on their workstation computers; the data must be saved on the server. Virus-checking programs are used regularly on HPSC computers, and appropriate e-mail and Internet use is stressed. The HPSC does not allow confidential data to be transmitted via e-mail.

Ms. Nelson explained that technical staff should be responsible for network security and should know how to install the appropriate hardware (e.g., firewalls, routers, encryption hardware, VPNs). Database administrators should have well-constructed databases and should not be using relational databases to store confidential data with public data in the same table. Keep up-to-date with hardware and software upgrades and patches. Have a backup system and disaster recovery plan in place. Management is responsible for instituting a culture of security and confidentiality. They have a responsibility to provide resources—developing and implementing a security plan is expensive. Managers have the ultimate responsibility for security and must assure that staff are trained and understand and support the proper use of hardware, software, and data.

MDH Policies and Procedures

Ms. Nelson discussed MDH security policies and procedures. Within her department, a large group of technical and program staff developed a policies and procedures manual. The manual meets the Division's needs and serves as a checklist. Ms. Nelson noted that executive-level buy-in is critical in these types of efforts. The MDH has a Data Practices Coordinator and Chief Information Security Officer on staff. In-house security evaluations are conducted on a regular basis, and all contractors and agents have to comply with MDH policies and procedures. It is critical to have system documentation to bring the system back up if it goes down. Ms. Nelson explained that the policies and procedures manual also covers firewalls, virus protection, VPNs, monitoring and auditing tools, encryption, access control and authentication, authorized hardware and software, remote access and electronic communications, physical environment, disaster recovery and backup, and user notification and training. The MDH has developed a Computer Incidents and Response Team that has crossdivision representation and responds to incidents as well as evaluates and modifies policies and procedures if necessary. Every employee at the MDH is trained in their security responsibilities. There is mandatory training on data practice responsibilities for staff who work with data. All employees are asked to sign an MDH Information Resources Employee Security Responsibilities Form.

Auditing

The MDH had an audit performed in the spring of 2000, which was not very effective because it was inconsistent. The audit conducted some penetration testing, and a few vulnerabilities were identified and addressed. The HPSC conducted a more thorough audit limited to the Encounter Project in the fall of 2000. The HPSC requested an audit from a respected firm, which was

provided with unlimited HPSC access and staff. The auditors conducted penetration testing both externally in a hacker mode and internally in an employee mode. They also ran physical and facility protection testing, analyses of data systems and internal documentation, and reviews of policies and procedures. The results were that the HPSC Encounter Project had tightly controlled access with a 10 million to 1 probability of having their encryption code broken. There were a few low-risk vulnerabilities identified related to labeling and the quality of passwords; these have since been resolved. The auditors concluded that the HPSC had a superior level of protection. Ms. Nelson explained that these results assured their management and their supporters that the data are protected and their system is secure. Results of the audit have been extremely helpful in legislative hearings and in cultivating relationships with existing and prospective data partners and supporters as well as with analysts and researchers. The results also have provided a viable defense with which to deflect/respond to attacks from critics.

Next Steps

Ms. Nelson indicated that the HPSC hopes to collect more personally identifiable data; conduct biennial audits, which is an expensive but worthwhile undertaking; and continue building constituencies. Issues and challenges include:

- **HIPPA.** HIPPA has three parts: (1) standards, (2) privacy, and (3) security. Standards allow for improved data definitions; however, its implementation has been delayed for 1 year. In terms of privacy, there are many exemptions for public health and oversight activities, and many registries may fall under that exemption (see HIPPA Subpart 164.512). The security section can be used as a blueprint for appropriate ways to use data.
- **Improvements in technology.** More effective security methods are always becoming available. They will offer a greater ability to access more data, match data across collections, and perform data management tasks faster. Improvements in technology also will lead to better hackers and more effective hacking tools, however.
- **Cost.** Security is expensive and requires staff time, hardware, software, databases, a network, and encryption. Responding to a security breach also requires a significant amount of resources. Too much security, however, decreases the ability to use the data.
- **More savvy general public.** Researchers used to be able to sit in their institutions and do work while no one knew what they were doing. Now there are privacy listservs, newsletters, and privacy advocates who are becoming organized. The media generally does not help the cause. If there is one bad incident in 15 million, that is the one that the media brings to the public's attention, because the exception is more interesting than the rule. It was recommended that registries try to cultivate relationships with science reporters in electronic and print media. The public is afraid that data will be collected for one reason and used for another—this misperception must be addressed.

- **Targeted research.** In the past, health researchers were seen as trusted entities, but with the spotlight on privacy, the view is different now. Researchers have to justify the collection and use of data, respond to how data are protected, and respond to the “so what?” question. There has to be some justification for the research.

In conclusion, Ms. Nelson recommended that cancer registries address privacy and security in a proactive manner. Policies and procedures should be developed that fit the registry’s environment. Train staff; build constituencies and support; and utilize resources in legislators, volunteer organizations, other states and state agencies, the federal government, private sector, and professional organizations. Anticipate and acknowledge critics, and be prepared to answer the “who,” “what,” “where,” “when,” “why,” and “how” questions.

Inventory of Best Practices Assurance of Confidentiality and Security

Dr. Holly L. Howe

In 1997–1998, the NCI convened a large panel of experts to explore best practices for data confidentiality in cancer research. Drs. Howe and Deapen were part of that group. The experts were separated into different research groups, including clinical trials, biological specimens, and surveillance. As a member of the surveillance group, Dr. Howe was shocked to learn that cancer registries were in some areas doing very poorly in adhering to basic confidentiality best practices. For example, some registries were sending confidential data via e-mail and over the Internet without encryption. This meeting served as a wake-up call.

In discussions with the NAACCR Board, Dr. Howe was asked to compile the Inventory of Best Practices Assurance of Confidentiality and Security (see Appendix A). This document is largely based on lessons learned from the NCI-sponsored best practices meeting. The intent of the Inventory is to help registries identify what best practices they are and are not following. It should help registries prioritize their “to-do lists” of actions to improve their security and data confidentiality protection processes. Dr. Howe and the Board agreed to wait until this workshop before releasing the Inventory so that workshop participants could identify any additional items to include in the Inventory to make it as comprehensive as possible. Workshop participants reviewed the Inventory during the breakout group sessions.

Breakout Groups

Workshop participants were divided into the following two breakout groups:

- **Registry Operations** (Deborah Bringman, Thomas Faris, Susan Gershman, Holly Howe, Charles Key, Yang Mao, Mary McBride, Stacey Neloms, Wendy Nelson, and Beverly Wilson).
- **Information Technology** (Toshi Abe, Dennis Deapen, Eric Durbin, Steve Fuschlin, Barry Gordon, Gary Hullet, Carol Kosary, Andy Lake, Thomas Taylor, and Warren Williams).

Ms. Knapp provided each breakout group with a template of questions that incorporated recommendations from CERT best practices, the Inventory of Best Practices Assurance of Confidentiality and Security, and IOS guidelines. The templates were structured as a series of questions relevant to either registry operations or information technology. The templates were utilized in some of the breakout discussions—in other breakout group discussions, the templates were reorganized or participants developed alternative formats with which to present their recommendations.

Registry Operations Breakout Group Recommendations

Physical Security Procedures for Confidential Data

Develop and maintain the cancer registry's nondisclosure and confidentiality agreements.

- Who is responsible for developing and updating the agreement? Ultimately, the Registry Director, with legal input. The agreement should be reviewed at least annually by the Registry's change committee.
- Who signs the agreement? Employees sign the agreement at the time of hiring; this includes students, volunteers, contractual workers, site visitors, and anyone who looks at the data, even on an *ad hoc* basis.
- How often should employees sign a confidentiality agreement? The document must be re-signed at routine intervals, at least annually, and could be timed with employees' annual performance evaluations. Having confidentiality agreement signed on a routine basis is helpful in terms of maintaining a culture of responsibility to protect the confidentiality of patient data. The agreements also should be re-signed every time registry's policy changes.
- What should be included in a confidentiality agreement? A confidentiality agreement must state the consequences of a breach. New hires must be provided with written security/confidentiality policies and personally review them. The agreement cannot include everything in a registry's security and confidentiality manual, but it should include a statement attesting to the fact that the person has read, understood, and is willing to abide by all registry confidentiality and security policies. The agreement also should state why it is important to maintain confidentiality so that the signer understands this. The individual's name (typed and signature), date, and signature and name of witness should be included. The witness must be the Registry Director or an individual designated by the Director to have signing authority. The confidentiality agreement should be limited to 1 page, written in standard English. Specific registry manuals that need to be reviewed should be referenced.
- What constitutes a breach? Any disclosure—intended or unintended—is a breach. The security must be very tight. Procedures vary widely for the authorized release of confidential information. A breach is the disclosure of private information in a public setting or in a situation where unauthorized individuals obtain private information. Breaches can occur when an individual overhears a private conversation, or when an individual looks over another individual's shoulder to see confidential material on their desk or computer monitor. Discussing patient data outside the office and after employment with the registry ends also constitute breaches.

- What are the methods for addressing a breach? Methods must include disciplinary action, including the potential for termination of employment.
- What are the methods for detecting and monitoring adherence? It is difficult to monitor confidentiality practices. Breaches in security can be detected and monitored. Proxies, such as effective security practices, can be monitored. Registries should create a culture that enforces the recognition and importance of confidentiality.
- How should signed confidentiality agreements be stored? In personnel files, and multiple copies should be made for distribution to: the employee, supervisor, and human resources department. It may be worthwhile also to have a separate file/central file for all signed agreements, including those signed by visitors to the registry. All copies of every signed agreement must be kept for historical and legal defense as well as to demonstrate the culture of the importance of confidentiality.

Develop and implement continuous employee training in confidentiality and data collection, processing, transfer, storage, and disposal (this refers to the confidentiality portion of these operations).

- Where are the employees being trained? One source may be a course offered online by the Office of Health Service Research Protection. The course addresses confidentiality, ethics, breaches, and so on. Registries also should have internal trainers—senior staff with the authority and ability to train others on confidentiality issues. NAACCR should sponsor a centralized training program to assist registry staff in training their colleagues. Continuous training on confidentiality and data security practices should be part of registry operations.
- Who develops the training program? Most training programs are being developed locally on an *ad hoc* basis. There may be an opportunity for a standardized approach with training provided by NAACCR. An Internet-based course could complement NAACCR-sponsored training.
- Who trains the employees? A specially certified person on the registry staff with the appropriate training to establish a culture of confidentiality.
- Who should be trained? Everybody who works in or with a registry, including IT staff or others in different organizational units.
- How are they being trained? Locally and through *ad hoc* activities, although currently there probably is not much training at registries on these issues.
- What are the subjects of training? Paper security issues versus electronic security issues; vulnerability; definitions of security, privacy, and confidentiality; detailed policy explanations; explanations of why confidentiality of cancer patient data is important; rules and tools for protection; and examples of unintentional breaches.
- How often should they be trained? At least once per year, and whenever new policies are instituted. All employees must complete the training within a specified time period after being hired.

Develop and maintain confidential data physical security monitoring and audits.

- Who monitors and audits the physical security activities? A security officer who will attend a NAACCR training program in which a prototype for security procedures (similar to what is presented at this workshop) will be presented. NAACCR should have an audit team or confidential committee charged with developing security procedures. This team

will be comprised of people working in registries to go on site visits and audit registries. The cost to registries should be minimal. Site visits could be carried out in 1–2 days. NAACCR could provide registries that pass with a certificate.

- Who controls the monitoring and auditing activities? NAACCR should oversee the training and auditing programs.
- How are the confidential data files being monitored and audited? Registries should be audited once every 3 years by NAACCR, but should submit an audit “checklist” to NAACCR once per year.
- What are the guidelines to be used in the monitoring and auditing activities? A “checklist” to be developed by NAACCR (e.g., the Inventory of Best Practices Assurance of Confidentiality and Security).
- How often should the physical security system be audited? Registries should be audited once every 3 years by NAACCR, but should submit an audit “checklist” to NAACCR once per year.

Develop and maintain disciplinary action as well as penalty and consequence rules and regulations of breach of data security and misuse of data.

- What are the rules and regulations? Disciplinary and performance evaluations should be utilized by registries. If an employee violates these rules and regulations, they should be disciplined. As part of the performance evaluation, registry employees should be evaluated based on how they adhere to a corporate culture of confidentiality. For minor infractions, employees may take “refresher courses” on corporate policies of confidentiality. NAACCR should develop rules for all cancer registries to adopt. Realistically, disciplinary procedures are designed by individual organizations. NAACCR could establish principles and guidelines, but the rules and disciplinary guidelines should be developed by the registries.
- Who is responsible for developing and maintaining such rules and regulations? NAACCR develops the guidelines, and the registry Security Officer or human resources department enforces disciplinary actions.
- Who is responsible for enforcing such rules and regulations? The Registry Director.
- What are the violation and breach consequences? Discipline and documentation of poor performance on the employee’s record.
- Can the rules and regulations be modified and amended? Yes, because the needs may change.
- How are such rules and regulations to be modified or amended? Registries must follow state rules negotiated between unions and state departments.
- Who can modify and amend such rules and regulations? Changes must include input from the union, human resources department, and the Registry Director.
- How often can such rules and regulations be modified and amended? Depends on the need—when the unexpected occurs, registries need to be able to respond.

Physical Data Security

Develop and maintain strict control of the access of the physical data files.

- Who should have access to the data internally and externally? (1) Registry staff who have a functional need to access the data for a job-related purpose, and (2) the reporting site.
- Who should not? Anyone not covered in the answer to the previous question.
- Are there any exceptions? Disaster recovery staff and administrative support (filing) staff.
- Who controls and monitors the data access activities? The registry's Security Officer and the database managing staff.
- How are the data access activities being controlled and monitored? Via hardcopy log.
- What kind of data can be accessed for external use/external recipients? Copies to reporters upon request, patients upon properly executed requests, and valid legal orders.

Develop and maintain strict control of the collection of the physical data files.

- Who collects the data? Registry staff (typically _____ [name of individual]).
- How are the data being collected? Through registry staff, mail, modem lines, and the Internet.
- What kind of data are being collected? Abstracts and pathology laboratory reports.
- What guidelines must be followed when collecting data? Use locking cabinets; never leave data unattended outside its storage facility; deliver data to their destination in a timely manner; never leave data exposed for inappropriate viewing.
- Who controls and monitors the data collection activities? The Registry Director and operations staff, as assigned.
- How are the data collection activities being controlled and monitored? Incoming data should be logged in, there should be routine internal audits, data should be logged at pickup and at delivery, and there should be verification of receipt.

Develop and maintain strict control of the processing of the physical data files.

- Who is responsible for processing the data after they are collected? Registry operations staff (typically _____ [name of individual]); contracted entity.
- How are the data being processed after collection? With vendor software or "home-grown" software.
- Who is responsible for processing any data requests from external recipients? Registry staff (typically _____ [name of individual]).
- Who is responsible for monitoring and controlling the data processing activities? The Registry Director.
- What guidelines must be followed when processing data for internal and external usage? Depends on the organization, and must be defined by the organization.

Develop and maintain strict control of the storage of the physical data files.

- Where and how are the data files being stored? In locked cabinets, with the potential for the records to be transferred to a type of electronic data storage to reduce space requirements.
- Who is responsible for organizing and maintaining the data storage facility? The Registry Director and operations staff, as assigned.
- Who is responsible for controlling and monitoring the data storage facility and activities? The Registry Director and operations staff, as assigned.
- How is the storage of the data files being controlled and monitored? In locked cabinets under the control of specified personnel; consider use of an access log.

Develop and maintain strict control of the disposal of the physical data files.

- Who is responsible for disposing of the unused data files? Operations staff (typically _____ [name of individual]).
- Who determines that a data file be disposed? Operations staff (typically _____ [name of individual]).
- What criteria are used to determine that a data file be disposed? Registry regulations.
- What are the guidelines for disposing of data files? The timeline should be controlled by state and federal laws. Data files should be destroyed (not recycled or otherwise disposed).
- Who is responsible for controlling and monitoring the data disposal activities? The Registry Director.
- How are the data disposal activities being controlled and monitored? Through disposal contractors' sign-off, internal audits, and/or employee sign-off.

Develop and implement continuous employee training in digital confidentiality and digital data collection, processing, transfer, storage, and disposal.

- What are the training goals? New hire orientation that provides a general overview of organization, general privacy, security, and confidentiality procedures; training in computer procedures; specific functional training; routine training evaluation; change control system; annual training and evaluation; employee training record system; any individual using a database system should review the Database Management System Manual.
- Who is responsible for developing such an employee training program? The registry's Security Officer should be appointed to oversee the privacy and security functions of all operations. That individual should coordinate the security/privacy training, possibly integrating it within existing registry training programs.
- Who is being trained? Everyone must receive training to some degree. The registry Security Officer should identify specific training requirements for each operational function.
- Who are the trainers? Existing training staff should be utilized. Privacy/security should be integrated into existing operations—not treated as a separate consideration.
- How and where do employees get the training? At existing training facilities or onsite if appropriate. There should be on-the-job training supervision for an introductory period.

- What kind of achievement measures should be employed? Training examinations or introductory on-the-job training supervision.
- Who controls and monitors the training activities? The registry's Security Officer or designee (i.e., training program coordinator).
- How are the activities to be controlled and monitored? Through internal audits and routine performance reviews.

Develop and maintain disciplinary action as well as penalty and consequence rules and regulations for breaches of data security and misuse of data.

- What are the rules and regulations? The registry's operating procedures, security/privacy handbook, security/privacy agreement, and requests from the registry's Security Officer.
- Who is responsible for developing and maintaining these rules and regulations? The registry's Security Officer.
- Who is responsible for enforcing these rules and regulations? Each employee's manager, registry management, and the registry Security Officer.
- What are the violation and breach consequences? As permitted by state law: immediate termination for serious, intentional breaches; review of insignificant and/or unintentional breaches; termination for repeated violations; and retraining for all violations. Registries should not implement a system that cannot be enforced. An unfulfilled discipline requirement may result in waiving the policy and potential discrimination litigation if it is later invoked.
- Who can modify these rules and regulations? The registry Security Officer.
- How often can the rules and regulations be modified and amended? Anytime, upon approval of changed and reasonable notice to all affected parties.

Electronic Data Security

Develop and maintain strict control of the system/digital submission/collection of the confidential data. Issues include different data sources/systems, electronic files sent via e-mail, health institutions and government death files, and Web files in different registries.

- The policy should be specific enough to maintain confidentiality, but general enough to allow for the latest technology that meets the standard.
- Who is responsible for developing and maintaining such a system? The registry's IT staff, with input from the data provider, their IT staff, and legal counsel, as well as (possible) input from other data collection agencies that use the same data. Who can submit digitally? What are the sources of the data collection? Facilities approved to submit data.
- Internally and externally, how is the data submitted digitally? What are the security measures and guidelines for digital data submission? Policies are needed to maximize file security, including ensuring data integrity using secure media and secure processes. Procedures will be specific to the submission method and file format. Proper labeling and characterization of the file is required (e.g., standard Registry Data Submission Form) and direct labeling of the file and medium.
- Who monitors the digital submission activities? The registry, with feedback to data providers.

- How are the digital submission activities being controlled and monitored? A registry staff member should be responsible for reviewing the security component of data submissions. Routine feedback on compliance with security procedures should be provided to data providers. There should be policies in place for additional followup for serious or repeated noncompliance.

Develop and maintain strict control of the system/digital processing of the confidential data.

- Who is responsible for processing the data after they are collected? This is an internal registry responsibility. Procedures may include internal processing or contracting the work under registry control. The registry should designate appropriate staff.
- How are the data processed after collection? Registries should have policies in place to: (1) confirm data integrity/verify that the data are what they are supposed to be, (2) confirm receipt of data to supplier, (3) maximize security at the processing step (access limited only to processors), and (4) log data. As a quality assurance measure, ensure that data sent back to the supplier for error correction follow standard data submission policy and procedures. Procedures for disposition of copies of files include: (1) retention policies—protection and archiving of original files, with limited access and logging of archiving; and (2) disposal policies—procedures for time limits and confirmation of disposal.
- Who controls and monitors the data processing activities? How are the processing activities being controlled and monitored? This is an internal registry responsibility. Registries should have a policy in place to ensure that access provision standards and policies are being followed. There should be a regular review of roles and responsibilities such as logging and auditing, and a regular reporting of accesses and access assignments. The control and monitoring of processing activities may be internal or outsourced, but should be in compliance with national and other standards.

Develop and maintain strict control of the system/digital transfer of the confidential data.

- Who is allowed to transfer data digitally? Assigned registry staff.
- Where can the data be transferred digitally? To entities approved to receive data via the registry use policy. Needs for data transfer (external) include: (1) the reporting facility may need to see the data; (2) between state data exchange; and (3) reporting to federal and other national organizations (e.g., NAACCR, CDC, other state agencies). Exceptions: no secondary use and no secondary parties.
- How are the data being transferred digitally? Registries should develop a policy that maximizes security and ensures data integrity via secure media and secure processes. Written requests and data file transfer forms may be used. Procedures should be specific to the submission method and file format. Proper labeling and characterization of the file is required (e.g., standard registry data transfer form and direct labeling of the file and medium).
- Who is responsible for the control and monitoring of digital data transfer activities? This is an internal registry responsibility and should be the registry staff member responsible for reviewing the security component of data submissions.
- How should the digital data transfer activities be controlled and monitored? Via: (1) routine feedback to data providers on compliance to security procedures;

(2) additional followup for serious or repeated noncompliance; (3) a policy that ensures access provision standards and policies are being followed; and (4) regular review of roles and responsibilities such as logging, auditing, and regular reporting of accesses and access assignments. Procedures in compliance with national and other standards may be internal or outsourced.

- What are the security measures and guidelines for digital data transfer? Policies are needed to maximize file security, including ensuring data integrity using secure media and secure processes. Procedures will be specific to the submission method and file format. Proper labeling and characterization of the file is required (e.g., standard Registry Data Submission Form) and direct labeling of the file and medium. Procedures will have to verify file contents before and after transmission.

Develop and maintain strict control of the system/digital storage of the confidential data.

- Who is responsible for developing and maintaining such a system? The registry, within the requirements of relevant law and with input from IT staff. Preferably, specific tasks will be carried out by designated registry IT staff.
- How and where are the data being stored? In a secure system and location under the registry's control. It will be necessary for the registry, working with IT staff as necessary, to define the database structure, access methodologies, and physical environment.
- What are the security measures and guidelines of digital data storage? These need to be provided by registry IT staff experts.
- How often are the data backed up? The registry should set policies and high-level standards based on security/data integrity concerns. Backups should occur regularly, depending on how often the data change and on the reliability of the system. Guidelines should be provided to IT staff to operationalize standards.
- How are the data backed up (i.e., what equipment/system is being used)? Guidelines should be provided by registry IT experts; both onsite and offsite backups are preferred.
- Who is responsible for backing up the data? Registry IT staff with adequate knowledge of the process.
- Who controls and monitors the data storage and backup activities? Registry IT staff.
- How are such activities being controlled and monitored? Via logging of data storage/backup activities and routine testing of backup procedures.

Develop and maintain strict control of the system/digital disposal of the confidential data.

- Who determines what digital data should be disposed? (1) State law, and (2) the registry, according to its mandate and standards to protect data confidentiality.
- How does one determine if the digital data should be disposed? (1) State law, and (2) the registry, based on standards to protect confidentiality.
- Who is responsible for disposing of the data? Designated registry IT staff or other IT staff under the direction of the registry (e.g., IT staff from an institution that houses a registry within itself).
- How are the data being disposed? Using guidelines on procedures for designated registry IT staff.
- Who controls and monitors the digital data disposal? Designated registry staff, preferably registry IT staff.

- How are the disposal activities being controlled and monitored? Via logging of the destruction process based on retention/destruction policies, including who, what, and when, and requiring written documentation of specific information.

Information Technology Breakout Group Recommendations

Software and Applications Security

Develop and maintain an inventory of software, including operating systems and applications. This machine-specific list, at a minimum, should include: information on the software versions (including patches), licenses, location installed, installer, and vendor.

- Who is responsible for developing and maintaining the machine-specific list for the IT software and applications? This task should be appointed by the registry's IT Director.
- Who controls and monitors this list? This task also should be appointed by the registry's IT Director, and Registry Directors and budget officials should know what is on this list.
- How is this list being controlled and monitored? The list should be updated every time software is added, changed, or removed. Periodic (perhaps annual) audits of the list are recommended. There may be software to assist registries with this (running event logs).
- Where and how is this list being stored? A read-only copy of the list should be saved as an electronic file in a well-documented location. A copy of this list that can be retrieved and updated by appropriate registry staff should be maintained at an offsite location.

Develop and maintain an access permissions policy for software to ensure strict control of digital access of the IT software and applications. Different levels of authority are required to run different applications.

- Who has permission to run each application? This is usually defined by role, not by individual. The Registry Director should be responsible for designating these roles.
- Are there any exceptions? No, as long as the list of applications is complete.
- Who enforces the access policies? Unclear, but there should be penalties for inappropriate and unauthorized access.
- How are the digital access activities of the IT software and applications being monitored? Consider using audits of who is using each critical application. Confidential database use should always be logged.

Develop and maintain an employee training program for the security policies/issues of each application. This includes specifying which applications employees can install.

- Who should be trained? Every person who uses any registry software.
- Who is responsible to develop and maintain the Employee Training Program for the use of software applications.
- Who does the training? This task should be appointed by the registry's Security Officer.
- What are the subjects of training? These may include: installation policies, access policies, basic awareness of confidentiality issues, chain of command education, knowing to whom questions should be asked, e-mail virus control policies, password policies, and policies on leaving workstations unattended but logged in. Both organization-wide

training and departmental or task-specific training should be utilized. Staff should be trained to avoid practices such as leaving disks on desks and taking unauthorized disks/equipment offsite.

- How often are the employees being trained? Frequently, perhaps every time security/confidentiality policies are updated. IT training and registry operations training may be combined. Great care must be taken to impress the sensitivity and confidentiality of registry data on employees.

Develop and maintain a digital disaster recovery system for IT software and applications. This policy may include a backup schedule for all servers and workstations, storage (onsite and offsite) of backup media, plan for complete recovery at an alternate site, predesignated backup server (each registry should decide what level of redundancy it can realistically implement). Backup software is available.

- Who is responsible to develop and maintain the digital disaster recovery system for the IT software and applications? This may require more than one high-level individual (e.g., Registry Director and IT Director) as well as a multitiered approach (e.g., desktop, network).
- Who controls and monitors such a system? The registry's IT Director.
- What exercises or tests, if any, are being utilized to ensure the success of this Disaster Recovery system? Backup media should be tested on an alternate drive/system.

Other related points to consider:

- Keep an updated virus protection program running on desktops at all times.
- Ensure that all e-mails are scanned for viruses.
- Firewalls (software and hardware) should be monitored for correct configuration.
- Network security includes firewall, data access, and user account issues. Various components of a network include routers, layers, switches, firewalls, remote dial in, FTP, and authentication for outside users. Which of these components can the registry control?

Network Security

Network infrastructure.

- Network infrastructure, including routers and switches, should be designed, engineered, and configured to protect data confidentiality.
- Employees should be trained and educated on the proper use of network equipment.
- Having separate servers dedicated to separate tasks is an appropriate goal for registries that are just getting off the ground. This will lessen the system's vulnerability.
- Unauthorized computers should not be allowed to attach to the local network.
- Control and access of data (offsite access, unattended office) need to be carefully monitored. Be aware that operating systems can be vulnerable to security failures.
- All of the above should be confirmed by an independent outside source (audit).
- Registries need to document policies and network topography.
- In and of itself, having a firewall does not ensure security—it must be configured to the particular connections that the registry wants to allow.

Data transmission.

- Transmissions of data to and from other agencies should always occur over encrypted connections or by only sending files encrypted with currently accepted standards for data encryption. This might include Web transmissions based on secure socket layers and appropriate levels of encryption (128 bit currently). Win Zip is not adequate.
- By design, the Internet is not a secure area. FTP must be with a login (never anonymous), and use either encrypted files or secure FTP.
- E-mail attachments must be encrypted to current standards. The same levels of file security apply to e-mail attachments. All e-mail attachments should be scanned for viruses using updated virus-scanning software.
- Only send data by e-mail if there is an authentication process in place at both ends.

Remote access.

- Internet access to machines or the network should be limited to machines dedicated for that purpose and should not have confidential data on them.
- Remote access should be limited and controlled—there should be no PC Anywhere-like access. VPN is probably the most secure approach.
- External logins need to have authorization to identify who is coming into the system. Some of these methods might be (from least secure to most secure): password, point-to-point, digital certificate, and VPN.
- There should be a strict time out period on external connections and lockouts after multiple unsuccessful login attempts.
- Be sensitive of security when using wireless connections.
- When introducing any new technology, recognize what risks are being exposed.

Internal network access.

- Assure that passwords expire after a reasonable time, are of an appropriate length, and so on (see CERT guidelines).
- The LAN Administrator should be responsible for setting password policies.
- Individuals are responsible for setting passwords that meet policy requirements.

Laptops/home computers.

- Use passwords to access the hard drive.
- Set the laptop BIOS so that it cannot boot from a diskette in case the laptop is stolen.
- For laptops that routinely store privileged data, there should be another level of security using a software package that requires login to that directory, so that the data in the directory are encrypted.
- Do not store confidential data on a home computer or a local drive on a computer at work.
- Make sure that the environment is secure if working from home.

Intrusion detection.

- How do you routinely scan for it, and what do you do if you detect an intrusion? Refer to CERT guidelines.
- Registries also should have written guidelines for addressing a detected intrusion based on how significant the breach is.
- In the name space of your IP address, do not include the name of your cancer registry.
- Monitor system logs for suspicious packets.

Internet use.

- Use caution when visiting Web sites.
- Be aware of hostile applications and viruses that can be associated with cookies.
- Follow appropriate Internet usage practices.
- One threat is hidden software that, unknown to the user, sends out information. Firewalls may not detect this.
- Web browsers can be set to control what is downloaded to the desktop.

Web site development.

- For registries that maintain a public Web site, consider not requiring users of the site to receive cookies, out of deference to the security needs of the registry's clients.
- A registry staff person should be actively ensuring that Web server patches are up to date.

Physical Protection of Hardware

Physical security.

- Dr. Key's presentation provided a very good level of physical security for a cancer registry and the physical protection of its hardware.
- At an overview level, maintain a detailed and complete IT hardware inventory list. This might not be an obvious step for Registry Directors or IT Directors. This step is a good place to start thinking about protecting a registry's hardware from intrusion.
- Who prepares the list and what elements, at a minimum, are recommended for inclusion?

Strict control of the physical storage of the IT hardware and access to the hardware.

- Again, Dr. Key's presentation provided some excellent examples.
- The ideal circumstances are a strictly controlled machine room for mission-critical servers, firewalls, routers, and key database storage.
- Access to this room should be tracked (ideally using a card key system) and monitored periodically for inappropriate access.
- It is important to have a semirestricted work space with sign-ins and visitors escorted throughout the premises to reduce risk.
- Laptops create the most serious issues and were addressed earlier.

Hardware maintenance.

- Control of hardware maintenance is critical.
- Maintenance should be included as part of a registry's physical security plan.
- Emphasize to registry staff the importance of not allowing inappropriate individuals access to registry hardware.
- Who controls and monitors the physical storage of the IT hardware and its facility?
- If laptops or other hardware must be sent out for service, ensure that there are no sensitive data on the machines.

Operations of IT hardware.

- These issues are similar to those associated with access to the hardware. Maintaining strict control of operations is key.

Disposal of IT hardware.

- Be cognizant of sensitive data on hardware designated for disposal.
- The individual(s) responsible for disposal of IT hardware should refer to specific guidelines from the funding agency/institution and requirements for the documentation of disposal. It is not as simple as just throwing the hardware in the trash.

Hardware training.

- Hardware training is necessary for everyone who has access to the equipment and/or its operation.
- Training should be very broad because the perspectives can vary ranging from Registry Director to IT Director, Security Officer, and the immediate or local supervisor.

Disaster recovery.

- Developing and controlling a disaster recovery plan is a difficult task and one that is largely the registry IT Director's responsibility.
- It is vastly different to have a recovery plan for a building being destroyed versus a recovery plan for one server crashing.
- It will be helpful to develop a cost-benefit plan to weigh how much it costs to get a registry back up right away versus how long the registry can afford to be down. This is a local decision based on money.
- Test the recovery plan in its entirety.

Other points that need to be addressed:

- Physical security of backup media.
- Some laptop data security issues such as passwords and encryption.
- Security of fax machines—faxes that receive confidential data should be housed in a secure area.

Discussion of Inventory of Best Practices Assurance of Confidentiality and Security

Workshop participants made three suggestions for additions to the Inventory: (1) in the Education and Training section, include an item on routine performance evaluation; (2) also in the Education and Training section, include an item on identification of retraining needs; and (3) in the Electronic Security section's disaster recovery plan item, add a statement on offsite storage of backups. These additions have been made to the Inventory of Best Practices Assurance of Confidentiality and Security (see Appendix A). The group discussed the nature of the relationship between the material covered in the breakout groups and the material in this Inventory. After refining material in the meeting summary, the summary and this Inventory will be compared to identify content that is in one, but not the other. The language of the two documents will be made consistent so that they complement each other, one as an educational document (the summary), the other as a checklist (the Inventory). The Inventory may work well as a preaudit checklist for registries and also applies to contractors such as geocoding services (IMS uses the Inventory as well).

Committee Discussion

Data Use and Confidentiality Committee members met on the last day of the workshop. Products to be developed as a result of this workshop were discussed. A practical document is planned that will provide best practices and serves as a model for cancer registry IT security, confidentiality, and operations so that individual registries can specifically implement these policies and procedures and do not have to develop them on their own. Many registries may not have the capacity to do this by themselves and should seek partnerships with other agencies so that they are not overwhelmed. Registries need to know that they can go to outside sources for help.

An important component of the document to be developed will be a discussion of building partnerships and finding resources and funding to implement the best practice guidelines. Registries typically are isolated organizations—isolation is not the solution for this set of challenges. One specific recommendation was for registries to examine how their state health departments transmit highly confidential HIV data, because that pipeline could be used to pass highly confidential cancer registry data as well. A title was proposed for the document: *Security and Confidentiality Guidelines for Central Cancer Registries*, with the two logical main sections of the document being registry operations and IT systems. Also, it was proposed that the document include a preface, the Inventory of Best Practices Assurance of Confidentiality and Security, a glossary of registry operations and IT terms, and resources and references. Gary Hullet provided a draft glossary of IT terms (see Appendix B).

The guidelines detailed in this document should include common-sense practices that should become second-nature activities for cancer registry staff, with the idea of having a blueprint for registry operations and IT staff to create a secure environment. Committee members noted that registries should have a detailed inventory of hardware, software, and network typology available in the event that their IT staff leave the registry. The end of this workshop will signal

the start of NAACCR activity in developing documents and examining the practices of other institutions in efforts to compile comprehensive best practice guidelines for security and confidentiality, with IT and registry operations components. A major challenge facing this effort will be to keep these guidelines current, because the technology is advancing at a rapid pace. It was suggested that NAACCR's IT Committee may be an appropriate entity to keep the document updated. Also, it was recommended that the NAACCR Board be asked to designate the Data Use and Confidentiality Committee as a standing committee rather than an *ad hoc* committee. It will be essential to review the mandates of NAACCR's IT and Education Committees to determine overlap between these two committees and the Data Use and Confidentiality Committee.

One way to publicize the document is through the *NAACCR Narrative*, which could include an article highlighting the document's important points. Other ways to advertise the document include presentations at meetings and holding training seminars. One suggestion was to contact the Program Committee Chair for NAACCR's Annual Meeting to see if the document can be highlighted in some capacity at the meeting. Another suggestion was for NAACCR to provide standardized training seminars based on this document for registry staff, particularly for registry IT Directors who could then train staff at their respective registries. It was noted that the first paragraph of any security plan needs to address what assets are being protected and from what types of threats. The typical registry may not think of it in those terms. Developing a draft document that addresses standards, additional information resources, and discussions of partnerships and funding options would be a tremendous step forward in helping to clarify higher level issues and guide future objectives and activities. A proactive mindset rather than a reactive mindset will be required.

Security documents from other institutions should be reviewed to make sure that NAACCR's document is as comprehensive and forward-thinking as possible. Polling cancer registries to determine how many of them even have an existing security plan also would be a valuable exercise. After a draft meeting summary is distributed to workshop participants, selected individuals should review the material and compare it with their own policies and note any information missing from NAACCR's draft. The CERT Web Site should be explored, and relevant material and hyperlinks should be collected. Committee members were asked to submit any relevant Web sites after reviewing the draft summary for inclusion in the formal document. Monitoring and providing security updates/bulletins was discussed as an activity that this Committee may want to become involved with as a service to cancer registries. A conference call for Committee members and workshop participants to further discuss these issues will be scheduled for mid-to-late April, after a draft of the summary is distributed.

Action Items

Note: When individuals were identified to carry out specific actions, their names appear in bold following those items. Those items to whom a specific individual was not assigned do not have a name following them.

- Write a passage in the document informing central registries that they should not attempt to implement the document's guidelines on their own. Many registries do not have the capacity, and should consider partnering with key people in other organizations like state health departments. Central registries need to know that they can go to other resources and form partnerships with state, federal, and private organizations for help. **Warren Williams**
- Write an introductory section laying the groundwork for the document with basic information about confidentiality and security. Possibly include Charles Key's definitions of the terms "security," "confidentiality," and "privacy." **Mary McBride, Charles Keys**
- Write a section on contractor compliance issues to include in the IT section of the document (see Appendix C). **Jacintha Knapp**
- Review the first draft of the document and compare it with the existing security policies of central registries to ensure the comprehensiveness of the document. **Charles Key, Deborah Bringman (focus on registry operations aspects); Gary Hullet, Ron Darling, Tom Taylor, Darlene Dale (focus on IT aspects)**
- Review the first draft of the document and compare it with NIH's IT security guidelines. **Carol Kosary**
- Review the first draft of the document to ensure that it complies with CDC's expectations for NPCR registries. **Warren Williams**
- Reference/review CERT and try to synchronize their recommendations with the document. Develop a directory of relevant hyperlinks. **Gary Hullet**
- Contact the Chair of the Program Committee of the annual NAACCR Meeting to see if this document can, in some capacity, be included in the meeting. Possibly generate an abstract for the meeting highlighting the progress made at this workshop and the purpose of the document. **Dennis Deapen**
- Collect definitions of terms for registry operations from Committee members and assemble a glossary of registry operations terms. **Rachel Jean-Baptiste**
- Supplement the IT glossary developed by Gary Hullet. **Carol Kosary**

- Determine, with the help of the NAACCR Board, whether the Data Use and Confidentiality Committee should become a standing committee rather than an *ad hoc* committee, or whether these activities should be assigned to the NAACCR IT and/or Education Committees.
- Use the *NAACCR Narrative* to help publicize the document and highlight the important points.
- Obtain other security documents from other organizations to ensure that NAACCR's document is as comprehensive and relevant as possible.
- Call central registries to determine whether they have security plans in place and if so, identify them.
- Synchronize the language, terms, and content found in the NAACCR Inventory of Best Practices Assurance of Confidentiality and Security with the language, terms, and content of the document being developed from this workshop.
- Explore how to obtain relevant IT security updates.
- Develop an acronym list.

Adjournment

Dr. Deapen and Lois Vogel

Dr. Deapen and Ms. Vogel thanked Committee members for their input and participation, and adjourned the meeting.

Appendix A

Inventory of Best Practices

Assurance of Confidentiality and Security

Name of Organization: _____

Date: _____

Effectively protecting the confidentiality of individually identifiable data requires uniform and comprehensive practices. Please indicate whether _____ (*registry/firm name*) meets the following best practices guidelines for security and data confidentiality.

General Confidentiality Practices

YES NO

- Employees sign confidentiality agreements.
- Confidentiality agreements with staff are signed on a routine basis at _____-month intervals.
- The security practices of the organization have been audited with no material findings.
- If material findings were noted, they have been corrected.
- Written and explicit institutional policies and procedures are in place to deal with breaches of confidentiality.
- Proactive methods are in place to monitor and detect the adherence to confidentiality protection procedures.
- Data submissions are fully protected against legal discovery, including subpoena and freedom of information inquiries.
- Organizational or institutional penalties for misuse of confidential data and breach of confidentiality by staff exist, are available in writing, and are enforced.
- Access to data files is restricted to specific project staff, and access by nonproject staff is not permitted.
- An individual is formally designated to assure compliance with established institutional standards.
- Specific sanctions for confidentiality violations can be imposed that include employee disciplinary action and any of the following: remedial training in confidentiality, loss of certification of competency in confidentiality, prohibition from future work with confidential data at the institution, and discharge.

Education

_____ (registry/firm name) can assure NAACCR that it:

YES NO

- Has developed and implemented education programs regarding confidentiality that include information about the lack of security inherent in faxing, e-mailing, and other electronic data transfer; reminders about not using names or other personal identifiers in conversations in public areas such as open laboratories, elevators, or hallways; and reminders to employees of their special duty to maintain confidentiality when research involves individuals they know personally.
- Formally credentials staff who have received confidentiality training.
- Performs routine performance evaluations.
- Identifies retraining needs.

Electronic Security

_____ (registry/firm name) has the following *technical practices* in place:

YES NO

- Authentication of users by means of passwords or digital identification.
- Access control by means of role-based authentication/access, locked server room, and an internal firewall.
- An audit trail that documents who, when, and for what purpose data (including paper) were accessed.
- A disaster prevention and recovery plan including adequate fire and entry alarms where data are stored, a fireproof file space for paper, routine backups of electronic data at intervals appropriate for the rate of data accrual, and offsite storage of electronic data backups.
- External firewalls in places to prevent remote access by unauthorized users.
- Virus checking is routine as are updates to the data files and engines to provide maximum protection of data files.
- System assessment including diagnostic runs and external audits are conducted regularly to ensure the integrity of the system.
- Data that are sent and received in conjunction with NAACCR activities are electronically encrypted.
- A data retention schedule is defined that includes a notation of the date when files are destroyed.
- Data file owners are notified when their file is destroyed.

The *transfer of data* is accompanied by:

YES NO

- A data-transfer agreement incorporating confidentiality standards to ensure data security at the recipient site and set standards for the data use at the recipient site.
- A paste (electronic) or stamp (paper) on all records containing identifiable data as a reminder of the need for special handling.
- Telecommuting and the use of home offices maintains the same level of security and procedures to address special issues, including data-transfer agreements, secure transmission procedures, and encryption. Additional safeguards also are followed, including: maintenance of minimal data on home computer, use of electronic screensavers, and password control at home.

Paper Record Security

_____ (*registry/firm name*) maintains the confidentiality of paper records by:

YES NO

- Restricting access to data-storage areas, the use of locked file rooms or cabinets in limited-access areas, a forms tracking log for any external disclosures, and a sign-out system for internal use of data.
- Developing and implementing policies by institutions for the secure transport of information from one physical location to another.
- Assuring confidentiality of written evidence that a patient is on a specific research study; for example, logs or lists of screened individuals or participants should not be left out on desks or in other open-access areas.
- Safeguarding ancillary records (e.g., pharmacy records, data on patients screened for clinical trials participation, etc.).
- Situating FAX machines in secure or limited-access areas; use of a precoded number to eliminate dialing errors; cover sheets so data are not physically exposed; testing FAX machines to ensure correct number and function; and deprogramming FAX memory storage after use to prevent recovery of confidential information.
- Employing established shredding procedures for disposal of documents after use.
- Protecting hardcopy information of sensitive information sent outside of the department.

Re-release of NAACCR Data Files

_____ (*registry/firm name*) does not release any NAACCR data files to anyone without written consent of the NAACCR Executive Director or the Chair of the Data Evaluation and Publication Committee.

A written consent is required every time a data request is received, even if the requester has obtained previous approval or if new data are added to a data file that was previously approved for release.

Signature

Typed Name

Title

Date

Appendix B

Draft Glossary of Networking Terms

Address

A method of uniquely identifying a host (or person) within an internet. Several address types exist within an IP environment namely the domain name, IP address, MAC address, and when referring to a person, an e-mail address.

American National Standards Institution (ANSI)

An American standards-making body responsible for the creation and approval of many standards in the United States. One such standard is X3T9.5, the standard describing FDDI.

American Standard Code for Information Interchange

A standard encoding scheme that is commonly used within the computer industry. ASCII (as it is commonly known) is based on a 7-bit scheme.

Anonymous FTP

Available on many FTP servers, anonymous FTP allows a user to gain access to public areas of the host without the need for a formal user ID and password.

Application Layer

The uppermost layer (Layer 7) of the OSI Model, this layer provides access to the network environment. Application protocols such as FTAM reside at this layer.

ASCII

American Standard Code for Information Interchange.

Authentication

A method by which a person (or process) can be identified. Several protocols within the Internet suite (such as PPP, RIP II, and OSPF) incorporate authentication methods.

Auto-Negotiation

An automated negotiation facility whereby IEEE 802.3 devices can negotiate the best possible connection. For example, in multiple technology device ports such as those found on typical 10/100 Ethernet Switches can support 10 Mbps, or 100 Mbps, at either full or half duplex. By using auto-negotiation, the device and port exchange information so that the best connection is established.

Bandwidth

Generally, this is taken to mean the amount of data that can be passed over a particular communications channel within a given time.

Bridge

A store and forward device, operating at Layer 2 of the OSI Model (the Data-Link Layer), and used to segment traffic between LANs. Also see Switch

British Standards Institute

The standards-making body responsible for approving standards applicable to the United Kingdom.

Broadcast

A packet or frame destined for all devices on a network segment or internetwork, a.k.a. a broadcast address.

Client

A system that requests the services of another. For example, a device requesting a file using the file transfer protocol is a client of the host on which the file resides.

Cyclic Redundancy Check (CRC)

Used in checksum calculations, the CRC provides the formula that is applied to the data as they are transmitted. Normally a polynomial function, the CRC is generated on transmission and checked on reception.

Dial-up

A method of communicating with a remote device over the Public Switched Telephone Network (PSTN). Such connections are therefore considered transitory rather than dedicated.

DNS

See domain name system.

Domain

There are many types of domain, such as a routing domain, named domain, and mail domain. In general, a domain can be considered as a group of entities sharing a common purpose.

Domain Name System

A host naming convention and protocol allowing the mapping of host names to IP addresses. The domain name system also allows other information to be stored about hosts and networks such as the location of mail servers, etc.

Electrical Industries Association (EIA)

A standards-making body in the United States responsible for the introduction of many data communications standards. The most common EIA standard is possibly EIA RS-232.

Electronic Mail (E-Mail)

The colloquial name for a system that allows network users to exchange messages. E-mail is one of the most common network applications.

E-mail Address

The address of an electronic mail user. Normally specified as a fully qualified domain name, this uniquely identifies a user anywhere within an internet.

Encryption

This is a technique that allows the octets within a packet to be modified in such a way as to ensure that any device eavesdropping will not be able to read the information. Data are encrypted by the transmitter and then decrypted by the receiver.

Ethernet

The original medium access system (developed by Digital, Intel, and Xerox) employing the CSMA/CD system. Ethernet defines a 10 Mbps Baseband signaling system, originally developed for use with coaxial cable. This has since been enhanced by the IEEE and now uses multiple media types including Twisted Pair and Fiber Optic cables.

File Transfer Protocol (FTP)

A protocol that allows users on one machine to transfer files to/from another.

Gateway

Within the context of the Internet Protocol Suite, a gateway is a router. In a more pure sense, a gateway normally translates application or other protocols. For example, TCP/IP to LAT allows a user running a Telnet session to attach to a LAT-based host, and vice versa.

Heterogeneous Network

A network that runs multiple network layer protocols such as IP, IPX, DECnet, etc. This is in direct contrast to a homogenous network where only a single protocol is employed.

Host

A device (normally a user device) that resides on a network.

Host Address (Internet Address)

The unique address assigned to a device on a network. Several addresses can be applied to a device namely a MAC Address (at layer 2), an IP address (at layer 3), or a name.

Host Name

A name given to a device that uniquely identifies it. Names within an IP environment are generally referred to as Domain Names.

Hub

A device that allows multiple network devices to intercommunicate. This may be a repeater (for Ethernet/802.3 devices), a *Multistation Access Unit* (for Token Ring), or a *Concentrator* (for FDDI). Alternatively, this may be a chassis that can comprise multiple LAN technologies.

Hypertext Mark-Up Language (HTML)

A language used to create pages of information used on the World Wide Web.

Hypertext Transfer Protocol (HTTP)

The protocol used to manipulate (upload and download) World Wide Web pages.

In-Band

The term used to describe the transmission of information (normally management information) along with normal user data. This is in contrast to *out-of-band*, where such control or management data are passed over a different channel.

Institute of Electrical & Electronic Engineers (IEEE)

An American standards body that is responsible for the introduction and standardization of many, now commonly used, network access methods.

International Standards Organization (ISO)

An international organization responsible for the introduction of many standards including those that are computer and communications related.

Internet

The worldwide network to which many businesses, educational establishments, government departments, and individuals now subscribe. The Internet (denoted by the capital I) is a collection of networks interconnected for the common goal of global communications.

Internet

An internet (denoted by a small i) is a collection of networks interconnected with routers and run primarily for private use. Also referred to as an *internetwork*.

Internet Control Message Protocol

A protocol that is considered as an integral part of IP used to report errors, and other information, and for rudimentary testing.

Internet Engineering Steering Group (IESG)

A group providing first-level technical review of all Internet standards and is responsible for the day-to-day management of the IETF.

Internet Engineering Task Force (IETF)

A large group of individuals, vendors, and researchers who are responsible for the evolution of the Internet protocols.

Internet Group Management Protocol (IGMP)

An integral extension to the Internet Protocol (IP) that allows host groups to be formed. This protocol then allows routers capable of multicast forwarding to determine where host group members reside and forward relevant multicasts to them.

Internet Protocol

The network layer protocol of the Internet Protocol Suite. The Internet protocol is a connectionless, best efforts protocol that relies on upper-layer protocols to provide reliability where required.

Internet Society

A society that provides the forum for discussion of the operation and use of the Internet.

IP Address

A form of host address applicable to the Internet Protocol Suite. In this address form, a 32-bit number (normally expressed in dotted decimal notation) is used to uniquely identify each host within the internet.

KERBEROS

A security system developed by the Massachusetts Institute of Technology (MIT) used to validate user access and using a system that encrypts data.

Local Area Network

A network that is designed to span no more than a few kilometers. Typically, these networks would be Ethernet, Token Ring, or FDDI networks and have data transmission speeds of up to 100 Mbps (*fast Ethernet*), or 1000 Mbps (*Gigabit Ethernet*).

MAC

See Media Access Control.

MAC Address

The hardware address of a device. Each device connected to a network technology such as Ethernet, Token Ring, or FDDI will have such an address that uniquely identifies it.

MAC Frames

A special type of frame used in technologies such as Token Ring and FDDI to aid in the overall management of the ring.

Mail Server

A host that distributes electronic mail items in response to requests from the electronic mail system.

Metropolitan Area Network

The term applied to networks designed to span campuses or other medium-sized areas. Obviously larger than LANs (yet smaller geographically than WANs), this describes an internet that covers a medium-sized area.

Network

A data communications system used to interconnect computer systems either locally or remotely.
See also local area network.
See also metropolitan area network.
See also wide area network.

Network Address

See also host address.
See also IP address.

NIC

See also network information center.
See also network interface card.

Point-to-Point Protocol (PPP)

A protocol used over serial point-to-point links to allow the transmission of multiple protocols.

Port

This has two meanings. First, some may refer to the physical connectors of a device as ports. Within a TCP/IP environment, however, the term is used to describe a demultiplexing value so that data destined for a particular application can be uniquely identified. Both TCP and UDP use the concept of ports for this purpose.

Repeater

A networking device that transparently propagates data from one segment to another. Repeaters are normally used to either increase network length or to increase the number of device connections.

Server

The name typically given to a machine that is used to provide resources to another host. These services may be file services, print services, or naming services as found in the domain name system.

Simple Mail Transfer Protocol (SMTP)

A TCP-based protocol used to transmit and receive electronic mail messages.

Simple Network Management Protocol (SNMP)

A protocol for managing network devices that originally was developed for the management of IP hosts. SNMP also can now be used to manage IPX devices.

Subnet

A portion of a network that shares the same network address as other portions. These subnets are then distinguished through a subnet mask.

Subnet Address

The part of an IP address that identifies the subnet on which the device resides.

Subnet Mask

A 32-bit mask which, when logically ANDed with an IP Address, masks off the host portion of the address.

T1

A U.S. standard communications facility used to carry data at 1.544 Mbps.

T3

A U.S. standard communications facility used to carry data at 44.746 Mbps.

TCP/IP

The colloquial name given to the Internet Protocol Suite, derived from the two major protocols, namely TCP and IP.

Telnet

The Internet suite Network Virtual Terminal (NVT) Protocol allowing a workstation to access network hosts as if it were connected locally.

Transmission Control Protocol (TCP)

One of the major protocols within the *Internet Protocol Suite*. TCP, as it is generally known, provides a reliable, connection-oriented environment over which applications such as Telnet and FTP run.

Tunneling

The process of encapsulating a foreign protocol within, say, an IP datagram so that it can be passed over an IP network.

Wide Area Network (WAN)

A network created to span large geographic areas normally over serial lines, and commonly via PTO circuits.

World Wide Web

A hypertext-based distributed information system based on a client-server model. With the explosive growth of the Internet, there are now countless servers offering information on just about any subject imaginable.

Appendix C

Contractor's Compliance Issues

- ❖ **Who they are:** Company/individual name(s), physical address, telephone and fax numbers.
- ❖ **Contact person:** The primary person responsible for the contract—usually the Contractor's Project Manager, Chief Engineer, President, or Pre- or Post Sales Manager. Include the contact person's name, telephone and fax numbers, e-mail address, and title.
- ❖ **Contractor expertise and experience:** For example, ABC Company is a system integrator that specializes in SAP and Oracle applications integration. They have been in the system integration field for 22 years.
- ❖ **Company roles and responsibilities:** This is best explained in the contract.
- ❖ **Duration of the contract:** Annual (e.g., February 1, 2002, to February 1, 2003), or indicate a specific date if the contract is based on a certain completion/deliverable.
- ❖ **Contractor security practices and policies:**
 - If the Contractor has remote access to the Client's site and stores the Client's data on their site, the Contractor must supply their security policy information, which may include (but not be limited to):
 - The physical/digital security of the equipment/network that is used for the remote access and storing of the Client's data. Issues to consider include:
 - Physical storage of the equipment (i.e., the server where the Client's data are stored). The router and the firewall are stored in a locked room that is monitored by a key card locking device. Only the Network Engineer, the System Administrator, and the IT Director have access to the room and the equipment.
 - If the Contractor stores the Client's data in a server, what platform/operating system is being used, and what are the physical and digital security policies pertaining to that server (i.e., who has access, who maintains it, where is it being stored, how is it being protected from internal and external intruders)?
 - Hardware/system allocation—each client is assigned an individual server. If this is not the case, what steps are taken to separate this client's data from other clients' data, and what safeguards to the system exist?
 - Remote access medium—what method is used for the remote access? Ideally, the Client should insist on a point-to-point digital line between the two sites such as ISDN, frame relay, or a T1 line.
 - Client's network availability—it is important to address what steps the Contractor takes to prevent network unavailability for the Client's employees and clients when the Contractor accesses the Client's network.

- If the Contractor's representatives work at the Client's site, the Contractor must take the following steps:
 - Supply a list of their representatives, including but not limited to names, roles/ assignments, and training/expertise.
 - Require their representatives to abide by the Client's security policies when working at the Client's site. This requirement should be included in the contract.
 - Explain appropriate roles and responsibilities to their representatives. The Client may want to consider insisting on a written acknowledgment signed by all of the Contractor's representatives who work at the Client's site.