7

SELECTED TOPICS IN INFRASTRUCTURE AND INFORMATION ASSURANCE

William V. Maconachy, Thomas Harper, Donald G. Marks and Terry Mayfield, Chair

Abstract Since 1994 and the explosive growth of the Internet, there has been a growing awareness of the need for more research and development activities directed at protecting networked information systems and those critical national infrastructures that are dependent up such systems. Within the U.S. this awareness sparked an increase in R& D planning activity and led to exploration of future R& D requirements. Viewpoints of Infrastructure & Information Assurance R& D planning activities (both past and present) were presented and some of the future requirements and planning activities that are underway to address them were discussed. Mr. Mayfield presented various aspects of the U.S. Federal Government's Infrastructure and Information Assurance R& D Program development. Topics included Infrastructure Assurance, High Confidence Systems, and Information Technology for the 21st Century. Further details of this presentation are included herein.

Keywords: Critical infrastructure protection

1. INTRODUCTION

The panel provided some illustrative infrastructure protection issues with a specific focus on the Telecommunications and the Electric Power Industries. Some of the remedial activities underway within the Electric Power Industries were discussed. Dr. Marks discussed issues in the Telecommunications Sector. The telecommunications (voice transmission) industry has been identified as one of the "critical infrastructures" in Presidential Decision Directive 63 (PDD-63). This industry is undergoing tremendous changes and seems to be merging with the information (data transmission) industry. This merger will bring great changes to both industries, although perhaps the greatest will be

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35508-5_22

V. Atluri et al. (eds.), *Research Advances in Database and Information Systems Security*

in the telecom business. These changes raise significant security issues and will require substantial research and investment by the industry to maintain the level of service currently enjoyed in the country. This talk concentrated on explaining the underlying forces causing these changes and the types of security problems that will emerge in the coming years. Dr. Harper presented the Department of Energy's Information Assurance Outreach Program. This is a Department of Energy program run out of the Office of Safeguards and Security. This program has been actively engaged with the energy sector to help raise their security awareness and help them improve their Information Assurance posture.

Information Assurance has long been recognized within its community of practitioners as being void of sufficient education and training. Literacy in IA is critically needed, especially among the administrators and users of our critical information infrastructures. This need has received a growing awareness since 1994 that extends beyond the community of IA practitioners. Commercial industry is beginning to compete for individuals with IA skills acquired through education or training. The need for a professional discipline with a full range of education and training activities is now clearly apparent. Dr. Maconachy discussed current national program plans for establishing and certifying a federal cyber workforce, which is firmly grounded in information assurance skills. Programs discussed included Centers of Excellence, scholarships for Service, IA Career field, and personnel certification. Further details of this presentation are included herein.

2. INFRASTRUCTURE AND INFORMATION ASSURANCE RELATED R& D AGENDAS (TERRY MAYFIELD)

Infrastructure and Information Assurance (I& IA) R& D at the Federal Government level does not happen just because someone comes up with a good idea or a clear need. Pursuit of I& IA-related R& D requires funding-and the means to get that funding is to provide a clear justification of what the funds will be spent on, why such spending is important, and what is intended to be produced. A key element in justifying R& D is the Research Agenda, providing the framework and details necessary for R& D funding proposals to be vetted and approved.

Significant activity within the U.S. Federal Government and through various external support groups has occurred and continues to occur in the development of various I& IA research agendas. Research agendas in these areas are being developed by, among others, a Presidential Commission, Presidential Advisory Councils, Inter-Agency Working Groups, the National Research

Council, and individual Agencies. Participants in the Presidential Commission on Critical Infrastructure Protection (PCCIP) included Department of Energy National Laboratories, National Security Agency, National Security Telecommunications Advisory Council (NSTAC), and the Institute For Defense Analyses.

Under the White House Office of Science and Technology Policy the National Science and Technology Council Committee on R& D has an Inter-agency Working Group further addressing the development of an Critical Infrastructure Protection Research Agenda as well as an Inter-agency Working Group addressing High Confidence Systems. The President's Information Technology Advisory Council (PITAC) has provided a proposed research agenda to advance the development and use of IT. The National Research Council recently published Trust in Cyberspace, a study that includes an examination of IA R& D as well as recommendations for future IA R& D. Finally, individual Federal Agencies, such as the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA), have been continually evolving and improving their IA R& D programs through the development of such R& D agendas.

We look at several of these agendas or their inputs to gain a broader understanding of where the IFIP 11.3 Working Group might place future focus. Specifically, we will touch on the IDA support to the PCCIP, the High Confidence Systems Research Agenda, and the President's Information Technology for the 21st Century (IT2) Initiative. Additional information on HCS and IT2 can be found at http://www.ccic.nco.gov.

2.1 IDA COMMERCIAL SECTOR STUDY

The IDA support to the PCCIP included a study of IA R& D in the commercial IT Sector. Among its findings, the study found that the commercial sector participants felt strongly that the government had a responsibility to support basic research in IA fundamentals. Such fundamentals include addressing:

- Protection Concepts & Principles
  - Availability
  - Integrity
- System Complexity Issues
  - System dynamics & adaptability
  - Composability
  - Security Economics

  - Intuitiveness

- Trust Concepts
  - Defining trust
  - Risk Management

The study further found that the commercial sector felt strongly about the federal government investing more in research to support system-level engineering. Included in this research were:

- System Architectures
- Heterogeneous Component Integration
- Secure Interoperability & Evolvability
- Applied Engineering Research
- System Assurance
- Standards

These two key research areas, fundamentals and systems-level engineering, should be conducted primarily through academe. They are key to providing educated and trained scientists and engineers to the commercial sector. Further, the engineering research should assist the commercial industry with a better understanding of how to develop their individual products to work more effectively and securely in large-scale systems.

Equally strong, the commercial sector indicated that they should be responsible for conducting most of the research associated with IA components and products. The federal government should fund industry to perform high-risk component research. Areas included in the latter are: Active Nets, Secure Nomadic Computing, and Secure Computing in the Network.

2.2 HIGH CONFIDENCE SYSTEMS

The Inter-Agency Working Group on High Confidence Systems works within the structure of the White House Office of Science and Technology Policy and its National Science and Technology Council. This effort, analogous to the European Union's Dependability Initiative, is to promote technology research that will provide predictably higher levels of system safety, security, availability, reliability, dependability, and survivability. The intent is to narrow the gap between expectations and delivered systems. It result of this research

should make the development of HCS less costly while achieving higher quality. Importantly, this research is necessary if federal agencies are to accomplish many of the performance goals contained in their strategic plans.

There are many compelling issues driving the need to address high confidence systems. These include:

- Growing dependence on computing throughout industries having safety-critical aspects.
- Consumer software and hardware used as components in safety-critical and life-critical applications.
- Higher risk related directly to higher degrees of integration driven by cost and performance.
- Computerization increasingly being used to achieve new functionality.
- Infrastructure systems (e.g., transportation, power distribution) operating at capacity.
- Continuing experiences in highly visible failures in large complex systems.
- Traditional regulatory practices which emphasize certification are not up to today's challenges.

The HCS research areas being proposed include;

- Specification
- Composition theory
- Analytic interoperability
- Programming languages
- Validation
- Modeling and simulation
- System-level concerns under nominal and adverse operating conditions
- Evidence and metrics
- Process
- Monitoring, detection, and accommodation

The HCS implementation strategy, which is still being developed, is expected to be carried out in four levels:

- Foundations
- Tools & Techniques
- Engineering & Experimentation
- Demonstration & Pilots

2.3 INFORMATION FOR THE 21ST CENTURY (IT^2)

This is a Presidential Initiative, in response to the PITAC Report of February 1999. It focuses activity on (1) long term IT research leading to fundamental breakthroughs in computing and communications; (2) advanced computing for science, engineering, and the Nation; and (3) research into social, economic, and workforce impacts of IT, and IT workforce education and training.

The research agenda of this Initiative includes fundamental R& D in the following areas:

- Software
  - Software Engineering
  - End-Use Programming
  - Component-based SW development
  - Active Software
  - Autonomous Software
- Scalable Information Infrastructure
  - Deeply Networked Systems
  - Anywhere, Anytime Connectivity
  - Network modeling and Simulation
- HCI and Information Management
  - Computers that speak, listen, and understand human language
  - Computer sensors that enhance human capabilities
  - An "Electronic" Information Exchange
  - Information Visualization
- High-end Computing

- Performance and efficiency improvement
- Computational Grid
- Revolutionary Computing

The Initiative also includes funding for "Expeditionary" Centers and for IT2 Enabling Technology Centers (ETCs).

The proposed five Expeditionary Centers (possibly virtual) would each have a different focus based upon assumptions not true today. They would have discipline-based or infrastructure-based themes and a goal of "mapping the future." Each of these centers would be performing activities in technology testbeds, economic and societal studies, education, and outreach.

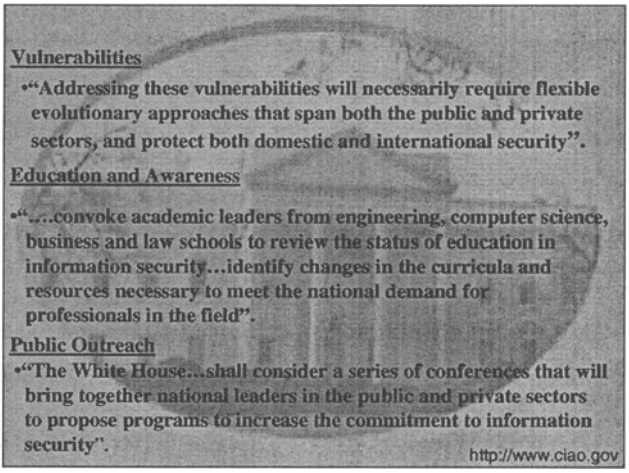

Figure 7.1 Critical infrastructure protection initiatives.

The proposed Centers of Excellence in Computer Science and Engineering Research would focus on applied technology and development. They would be integrated environments at universities and Federally Funded R& D Centers (FFRDCs) applying next-generation IT to important national problems. These ETCs would perform several functions including:

- Education and training

- Testbeds
- Research on factors inhibiting development of IT in the application domain
- Community building

In summary, a lot of Federal R& D program development activity is underway. Goals include:

- Advancing IT capabilities by orders of magnitude
- Increasing confidence in systems
- Protecting critical national infrastructures
- Applying next-generation technologies to national problems
- Focusing I& IA related R& D efforts at the fundamental and systems engineering levels.

There is a strong recognition for the need of universities to play a key role in both I& IA research and education. And, there is a recognized need for improved government-industry-academe partnerships to achieve the R& D specified in these agendas.

3. TELECOMMUNICATIONS SECURITY AND FRAUD (DONALD G. MARKS)

Information and Communications (I& C) makes up one of the critical sectors defined by the Presidential Decision Directive # 63. Indeed, information and communications capabilities are critical to the proper functioning of all the other sectors. For example, the electric power grid depends upon a communications network to properly control the various hardware/software features necessary to function. The Department of Commerce has been named the lead agency for the I& C Sector, with NIST providing significant leadership in the research directions.

The most significant current trend is the merger of the telephone system with the computer network system to supply either voice or data over the same network. In fact, the Telecommunications Industry is in a state of flux and undergoing changes perhaps greater than any other critical infrastructure. Competition has opened telecommunications networks to new opportunities for service providers. In particular, the technique of transmitting digitized, packetized, voice presents many opportunities for new services integrated with the Internet or other existing computer networks. Unfortunately, the integration of the

Public Switched Network and the Internet also opens the telephone system to all the attacks currently only visited upon Internet sites.

In the interest of stimulating competition, the traditional telephone exchange carriers can now be required to allow new service providers to connect to their equipment and databases in the existing telecommunications network. Many of the new services being offered depend upon digital communication rather than requiring voice-grade, switched connections. That is, services such as automatic call forwarding, conference calls, or even no-toll 800 service, depend upon digital computer processing to provide the service. These digital computers may be resident anywhere on the Internet, they are not limited to the telephone company offices. The telephone companies may even institute differing quality of service options in the near future. For example, a "voice-grade" call may require a dedicated switched circuit while a packet-switched circuit may be sufficient for data calls. Since digitized voice packets are indistinguishable from digitized data packets, the network switching and routing software must be sufficiently intelligent to make these decisions.

The new telecommunications network, therefore, represents a hybrid model, with the packet switched Internet computers providing decision-making capabilities for connections between established, circuit-switched telephone lines. Services such as billing, connecting, routing, or call announcement (i.e. ringing) may all be essentially completed outside the traditional network, using the more flexible Internet connections. This emerging network is referred to as the "Next Generation Network" or the "Advanced Intelligent Network" within the telecommunications industry. These services will eventually become critical to commercial business models and reversion to previous telecommunications models will not be acceptable.

While telecommunications companies have traditionally been interested in fraud control, the new operating paradigm includes significant threats to service availability. That is, not only is fraud a potential problem, but destruction of vital data and network services is now easier, since critical services are resident on globally connected, Internet computers. Such vandalism could disable the system, with even more serious consequences than simple fraud. In addition, even fraud becomes easier due to the distributed network architecture and connection to the Internet.

Protection of this emerging distributed system requires adopting some security techniques that are common in network security, but relatively rare in the telecommunications industry, such as strong authentication, auditing, access control, and the use of security capable, perhaps even evaluated, system components.

The evolving Telecommunications Industry promises a cornucopia of interesting problems for database security experts. The system operates as a

distributed database resident at various locations on the Internet. The connection of a telephone call (i.e. a transaction) requires decisions at many different locations throughout the network. Competitors are required (by law) to allow access to databases - a situation very similar to an MLS (Multi-Level Secure) database. The major change will be an emphasis on data integrity (to combat fraud) and on reliability rather than confidentiality.

The Next Generation Network of the telecommunications industry may be the next "killer app" to demonstrate the necessity of database security procedures and techniques.

4. INFRASTRUCTURE ASSURANCE OUTREACH PROGRAM: INFORMATION ASSURANCE FOR ENERGY INFRASTRUCTURE OPERATIONS (THOMAS HARPER)

4.1 INTRODUCTION - INFRASTRUCTURE ASSURANCE OUTREACH PROGRAM

Over the years, the Department of Energy (DOE) and the National Laboratories throughout the DOE complex have invested in technological approaches to solve the challenges of protecting the nation's most sensitive information and special nuclear materials. As a result, significant expertise has been amassed for protecting national security interests. Much of the protection capability developed by the National Laboratories has application to industry as well as to government. Numerous advances in information security and assurance have been attained. Significant breakthroughs have also been achieved in the protection of automated information systems and the information they store, process and transmit.

The DOE Office of Safeguards and Security Infrastructure Assurance Outreach Program (IAOP) is intended to return to industry and the public the technologies and strategies borne out of many years of investments in the protection of the nation in response to the Cold War. The IAOP offers the following in support of providing protection for the Nation's infrastructure:

- **Technology Sharing:** making available various high and low technology solutions to industry.

- **Advice and Assistance:** standing ready to assist in the conduct of specialized assessments intended to identify threats and vulnerabilities and provide advice regarding appropriate approaches regarding countermeasures.

- **Information Resource:** providing useful information through published reports, analyses, studies, and World Wide Web sites.

The IAOP serves as one facet of a number of programs that DOE employs to discharge the responsibilities required by Presidential Decision Directive 63. PDD-63 charters federal agencies to assist critical infrastructure industries with the enhancement of their security posture. The DOE is responsible for energy sector infrastructures such as oil, gas and the electric power grid. In this presentation, the focus is on the electric power industry.

4.2 IAOP ASSESSMENT ACTIVITIES

The IAOP provides assistance to industry by assessing the infrastructure assurance aspects of an installation's information infrastructure. An important function of the assessment activity is to raise the level of awareness within the industry regarding information assurance issues. Typical assessment activities include:

- **Asset Mapping:** Utilizing a combination of industry specific domain expertise and infrastructure assurance / information security experts, assets critical to system operation are identified and the consequences of component failure are catalogued.
- **Network Architecture:** The architecture, components and operation of the communications infrastructure are evaluated for vulnerabilities. Other issues, such as configuration management and host-based security systems also are addressed.
- **Penetration Testing:** Active "white hat" attacks are made on the client installation to map and validate vulnerabilities.
- **Threat Environment:** An evaluation of threats that may potentially be arrayed against an industry and/or installation is compiled. Staff awareness of the threat environment is assessed.
- **Physical Security:** All physical aspects of security and their relevance/impact to the information infrastructure are evaluated.
- **Operations Security:** OPSEC is a process by which an organization denies pathways that could allow adversaries access to sensitive information. This process includes the identification, control and protection methods for sensitive information.
- **Policy and Procedures:** Review of policies and procedures relating to security and assessment of their effectiveness. Staff awareness of policies and procedures is also evaluated.

- **Energy System Influence:** Assess the capability for a skilled person to manipulate a power industry entity through secondary effects such as "gaming" the market.
- **Risk Analysis:** In this phase, threats, vulnerabilities and critical assets are analyzed and reported to the client.

A second phase of the IAOP assessment methodology includes follow-on activities such as tool and technology transfer, assistance designing and implementing countermeasures, training, etc.

Assessments have been completed or are underway for a number of electric power entities including:

- California Independent System Operators (ISO)
- Western Electric Power Exchange (WEPEX)
- Texas Utilities
- North American Electric Reliability Council (NERC) Interregional Security Network (ISN)
- ISO New England (In Process)

4.3 TRENDS

Across the electric power industry, there is increasing infrastructure dependence on information. Deregulation and market forces are strong drivers influencing the industry to leverage technology and develop cost effective, automated systems. Standardization, particularly in the networking arena, is making it possible to combine functions that have historically been separated. This information-centric trend has led to an increased interdependence among various systems and increased the breadth of potential impact in the event of an infrastructure compromise.

Also, the electric power industry is restructuring. The "downsizing" trend has left fewer infrastructure staff and increased dependence on information. As part of deregulation, there are open access requirements, mandated by law. There is a move to standardize on "open systems" for maintainability and cost reasons. And as the market for brokering electric power has begun operation, there is increased competition and focus on cost control.

There are infrastructure issues unique to the Energy sector. Supervisory Control and Data Acquisition (SCADA) systems can gather information and provide control signals to remote systems as part of the Energy Management System (EMS) and/or Power Control System (PCS). For example, as pressure

increases to reduce cost and consolidate systems, critical control signals may be routed over non-dedicated communication channels.

Taking these trends together, it becomes apparent the industry is moving into a new age. With fewer trained staff, financial pressures requiring an increased utilization of assets, infrastructure systems are becoming highly interconnected, and information gaining importance as a tool for competitive advantage, new businesses and models of operation are appearing in the industry.

4.4 SUMMARY

Information has increased in importance in the electric power industry and this upward trend should continue for the foreseeable future. The stability of the power grid is now interwoven with the information infrastructure within the industry. The IAOP has actively been supporting this critical infrastructure industry address these issues through assessments, technical assistance and education.

5. THE HUMAN DIMENSION OF CYBER PROTECTION (WILLIAM V. MACONACHY)

Information Assurance (IA) encompasses many disciplines that, when practiced in concert, help to ensure the availability, integrity and confidentiality of information and information systems. Failures of those systems and increasing attacks on those systems necessitate a new "Corps" of cyber security-savvy professionals. The U.S. Government's response to this need for a cyber corps is rooted in a 1997 report of The President's Commission on Critical Infrastructure Protection.

The Commission determined "that the nation is so dependent on our infrastructures that we must view them through a national security lens." The Commission recognized that there is a growing cyber dimension associated with infrastructure information assurance - - our critical infrastructures have no boundaries, thus our infrastructures are exposed to cyber vulnerabilities and cyber threats. Our past network defenses offer little protection to this cyber threat.

In response to that report, The President issued a Presidential Decision Directive, which states, In part:

> It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. I intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

These words from the White House accent the grave nature of our cyber vulnerabilities.

These words are "enablers":

- They enable government agencies to move together in reaching out to government and private sectors in search of Information Assurance solutions.
- They enable government to move forward without haste in seeking and fielding Information Assurance solutions.
- They act as a charter and challenge to all segments of our society to build bridges not walls (UNLESS THEY ARE, OF COURSE, "FIREWALLS").

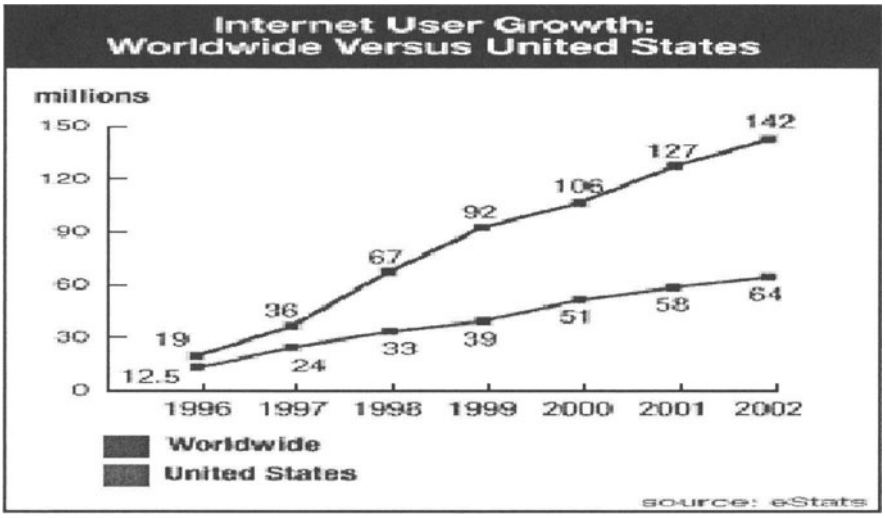

Figure 7.2 Internet user growth.

As shown in Figure 7.2, the explosion in the use of the Internet brings with it added security challenges. In a time when demand for Information Assurance professionals is highest, the production is nearly at its lowest levels. A U.S. Department of Commerce report recently noted that between the years 1996 and 2006, there will be a need, in the U.S. for 1.3 million new information technology (IT) workers. Yet, U.S. institutes of higher education are only producing about 1/3 the number of skilled IT workers required to fill those new positions. In the computer science area alone, "the number of computer science/ computer engineering degrees awarded at the bachelor level fell from

51,231 in 1997 to 37,951." In this one IT field alone, America is experiencing a dramatic shortfall of qualified personnel. Extrapolating the need for IA personnel from the known shortfall in IT personnel, the national situation becomes more dramatic.

In response to this, the National cyber defense plan called for in Presidential Decision Directive 63 that is currently under construction has several components to the Federal Information Technology Service Section:

1. Federal Cyber Service;
2. Centers for IT Excellence (CITE); where an emphasis on researching best practices will be placed;
3. Scholarships for federal service program;
4. Awareness and literacy program for reaching secondary schools; and
5. A federal occupational study.

When fully operational, this program will define the performance requirements for information technology security experts and will infuse appropriate IA skills into other IT career fields. Another promising program is the NSA Centers of Academic Excellence in Information Assurance Education effort.

Launched in November 1998, this program encourages universities to examine their Information Assurance Curricula, and campus IA posture, against a set of national standards. In our first call for submission, applications were received from those universities having the most mature IA/INFOSEC education programs. Part of the criteria used in judging the applicants were the NSTISSC training standards. As you know, these standards were originally designed for use in the classified community. The submissions from the universities indicate that the standards have a more universal applicability, and also serve as yet another independent validation of the content of those standards.

This program will assist all private and government sectors in meeting increased national demand for a cadre of professionals with information assurance expertise in various disciplines. This is truly an example of information sharing between sectors of our society

Finally, on a truly national level, a consortium of industry, government and academia has been founded to promote IA in higher education. This multidimensional group is a focus area where industry, academia and government better communicate. Next year's conference will be hosted by The Office of the President in Washington, D.C.

In summary, within the borderless cyber world-nothing stands between the information assets in our critical infrastructures and those who would bring

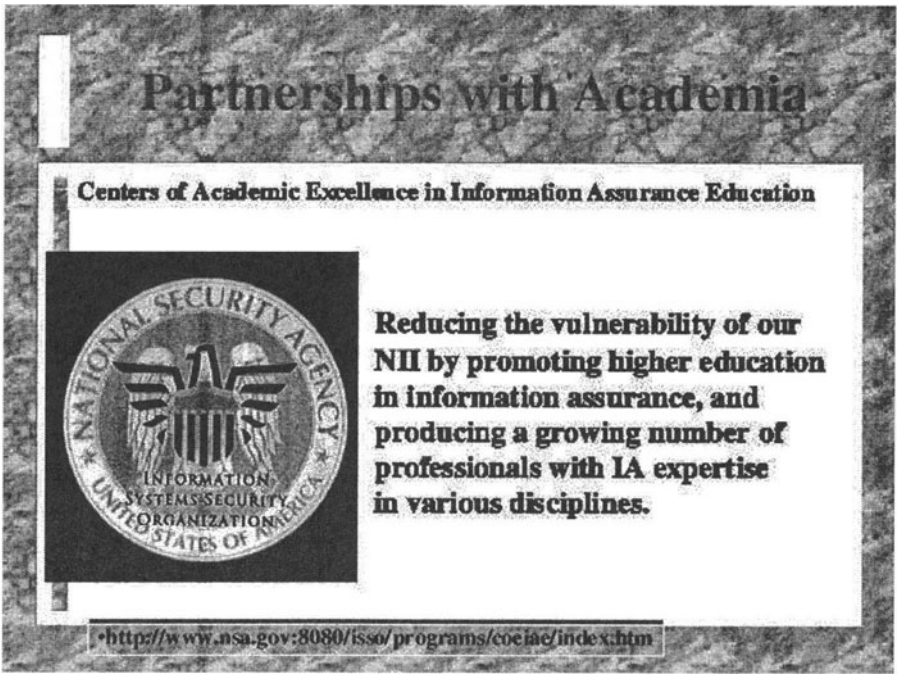

Figure 7.3 Centers of Excellence for Information Assurance Education Program.

those structures down. This increased threat calls for new directions and new pedagogic models in our educational systems. Educational systems at all levels must be able to respond to systems intrusions, misuse, and abuse by providing both initial and refresher education and training in all areas of information assurance.

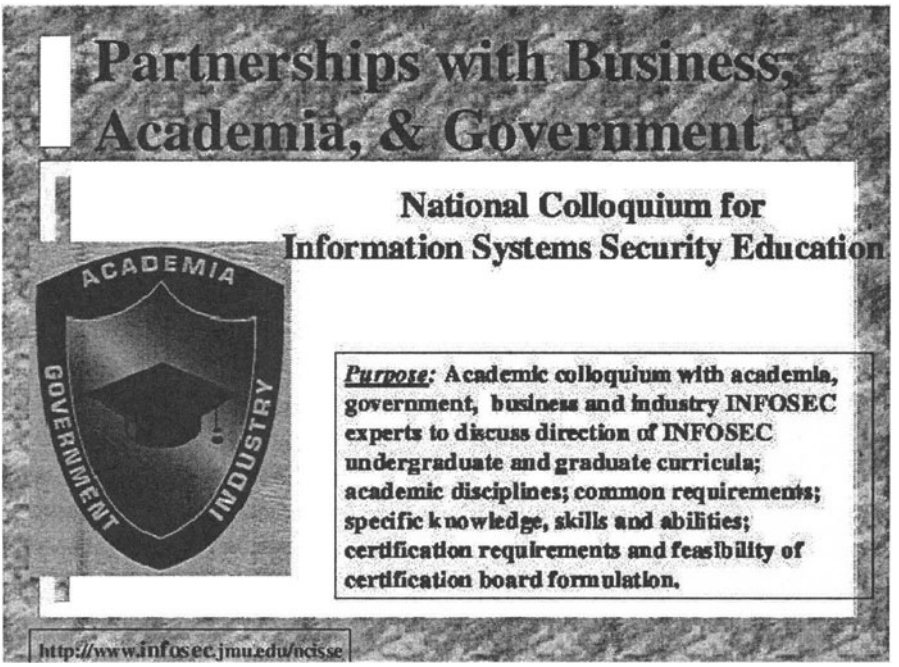

Figure 7.4 Industrial, academic and government partnerships.