REPORT OF

THE JOINT COMMISSION ON TECHNOLOGY AND SCIENCE

TO THE GOVERNOR AND
THE GENERAL ASSEMBLY OF VIRGINIA

REPORT DOCUMENT NO. 11

COMMONWEALTH OF VIRGINIA
RICHMOND
2005

MEMBERS OF THE JOINT COMMISSION ON TECHNOLOGY AND SCIENCE

Delegate Joe T. May, Chair
Senator Stephen D. Newman, Vice Chair
Delegate Kenneth C. Alexander
Delegate John A. Cosgrove
Senator Janet D. Howell
Delegate Sam A. Nixon, Jr.
Delegate Kenneth R. Plum
Delegate Harry R. Purkey
Delegate Thomas D. Rust
Senator Kenneth W. Stolle
Senator William C. Wampler, Jr.
Senator John Watkins

Director
Mitchell F. Goldstein, Esq.

Staff Attorney
Eric Link (through August, 2004)
Elizabeth J. Wallmeyer (Setember, 2004 -)

Senior Staff Assistant
Lisa Gilmer

EXECUTIVE SUMMARY

Created by the 1997 General Assembly through House Bill 2138, the Joint Commission on Technology and Science (JCOTS) is a permanent legislative commission charged to study all aspects of technology and science, to promote the development of technology and science in the Commonwealth of Virginia through sound public policies, and to report its findings annually to the Governor and the General Assembly (See Chapter 11 of Title 30 of the Code of Virginia, § 30-85 et seq.).

JCOTS' 2004-2005 work plan identified four issues for study through the establishment and work of advisory committees co-chaired by JCOTS members: Computer Crimes, Integrated Government, Nanotechnology, and Privacy. The work plan also identified new issues to be introduced at Commission meetings through testimony and presentations -- computer forensics and computer security -- as well as other issues to be monitored throughout the year, including privacy of personal information in court documents, taxes on Internet sales, and biometrics on identity cards.

JCOTS adopted the findings and recommendations of its advisory committees and submitted them to the General Assembly for consideration.

Joint Advisory Committee on Computer Crimes

JCOTS and the Virginia State Crime Commission combined their studies of the Computer Crimes Act and created a Joint Legislative Task Force and a Joint Advisory Committee. The Joint Advisory Committee on Computer Crimes was charged with examining the statutory basis for computer crimes and related laws in the Code of Virginia, including a determination of the appropriate definitions and elements constituting offenses, and recommending any necessary amendments in light of modern activities and technologies. The Committee and Task Force received briefings on the history of computer crimes legislation in the Commonwealth and the structure of the Computer Crimes Act.

Concerned that defining the specific threats would lead to almost immediate obsolescence and would provide a road map to the bad actors, the Task Force and Advisory Committee agreed to focus on the "bad actors" with a "bad motive" that do a "bad action." They identified nine specific threats: (i) phishing, spoofing, and disguising one's identity; (ii) bots and zombies; (iii) spyware and adware; (iv) viruses and worms; (v) falsifying certifications, seals, or other credentials; (vi) spam; (vii) identity theft; (viii) hacking and defacing websites, networks, and databases; and (ix) denial of service attacks. The Task Force and Advisory Committee focused on those threats not already covered in the Code.

The groups condensed and simplified the definitions, basing many of them on those of the Uniform Computer Information Transactions Act. Not wanting the Act to treat all devices with computer chips as computers, the Task Force voted to limit the coverage to general purpose, programmable computers. The proposed bill also requires that a person actually know or have reason to know that he was without authority, as opposed to merely acting without permission or right. Mitigating the impact of this final change, the crimes of computer fraud and personal

trespass by computer would no longer require that a person take the underlying actions without authority.

To handle bots and zombies, the bill adds a provision to the computer trespass statute that criminalizes installing software without authorization. The bill also adds a subsection to address viruses and worms that do not harm computers, but hinder their ability to operate peripheral devices (e.g., grocery scanners, security cameras, and environmental sensors). In addition, the bill addresses using a computer to obtain computer information without authority. Finally, to avoid criminalizing innocent or innocuous activities, the Task Force added a requirement that for an act to be actionable as Computer Trespass, a person must act with malicious intent.

The Computer Crimes Act criminalizes invading another person's computer, stealing information, and examining certain personal information without authority. However, in recent years, the phenomena of phishing and spoofing, or faking an identity to gather personal information, have tricked people into revealing the information themselves. In some cases, perpetrators trick computer users into downloading software that takes the information automatically. Therefore, the proposal criminalizes using a computer with fraudulent intent to obtain, access, or record identifying information, as defined by the identity theft statute (excluding name and birth date). Just trying to trick someone into revealing identifying information would be a crime; actually tricking them is not necessary.

The proposal also specifically criminalizes using a computer to circumvent computer security measures. Finally, it clarifies that all property regardless of type can be stolen or embezzled.

Though JCOTS expressed concern over the number of new felonies created by the proposal, it adopted the proposal as drafted by a vote of four to one with one abstention.

Advisory Committee on Integrated Government

The Advisory Committee on Integrated Government was charged with exploring the issues created or enhanced by the transformation of government in the electronic age. The Committee continued focusing on the state of information technology (IT) procurement in the Commonwealth, including briefings on the Virginia Information Technologies Agency's (VITA) Project Management Division and VITA's procurement reform efforts. In addition, the Committee received briefings on and discussed certified electronic mail, electronics recycling, the development of the Commonwealth's strategic plan for communications interoperability, and outsourcing and offshoring. Finally, the Committee addressed competing provisions dictating electronic meetings requirements for public bodies.

The Committee voted to recommend four proposals introduced by VITA. The first would eliminate a preference in the Virginia Public Procurement Act for competitive sealed bidding over competitive negotiation. The second would allow public bodies to purchase information technology and telecommunications goods and services from online public auctions and through cooperative procurement arrangements with approval of the Chief Information Officer. The third would authorize VITA to conduct an Alternative Dispute Resolution Pilot Project. The

final would allow public bodies to hold closed meetings to discuss records already exempt from public disclosure relating to the Public-Private Education Facilities and Infrastructure Act.

Finally, the Committee discussed JCOTS' Pilot Project, an exemption to the Virginia Freedom of Information Act that applies to meetings held via videoconference. The Pilot Project is due to sunset on July 1, 2005. Working with a FOIA Council subcommittee, the Committee proposed reconciling the provisions in the Freedom of Information Act and the Acts of Assembly to create one set of requirements for electronic meetings. However, unlike the FOIA proposal, the Committee proposed retaining the current Acts of Assembly provisions that enable a quorum to be distributed across remote sites and do not require that remote sites be open to the public.

Believing that procurement reforms beyond technology were outside its mandate, JCOTS declined to adopt the Committee's first proposal that would eliminate the preference of competitive sealed bidding over competitive negotiation. JCOTS conformed the electronic communications meetings bill to the FOIA Council proposal by retaining the current FOIA requirements for a physical quorum and remote sites open to the public. JCOTS adopted the remaining recommendations without amendment.

Advisory Committee on Nanotechnology

Pursuant to House Joint Resolution 120, JCOTS established the Advisory Committee on Nanotechnology and charged it with identifying nanotechnology research and economic development opportunities for the Commonwealth and considering the efficacy of creating a statewide, comprehensive and coordinated strategy to secure additional federal research and development funds and to boost commercial activity. Nanotechnology presents major new economic development opportunities, especially with the federal government's recent authorization of almost $3.7 billion in government funding for research and development. The Committee received briefings on an overview of nanotechnology, on other states' and the federal government's approaches to promoting nanotechnology development, and on a proposed prototyping facility that could help to bridge the gap between basic research and the commercial market.

While the Committee made no formal legislative recommendations, it focused on three key areas: commercialization (bridging the gap between research and commercialization), education, and financing (including business development and incentives). The Committee agreed that the Commonwealth should establish a more permanent body to continue discussions about nanotechnology in the Commonwealth. Adopting this recommendation, JCOTS agreed to include nanotechnology in its 2005-2006 work plan.

Advisory Committee on Privacy

The Advisory Committee on Privacy was charged with (i) reviewing current privacy laws and practices as they pertain to information and (ii) proposing policies and guidelines for public bodies to evaluate the use of potentially invasive technologies when determining whether to support their use financially or to authorize or prohibit their use. To evaluate the use of potentially invasive technologies, the Committee received briefings on a number of technologies,

including facial recognition, radio frequency identification, and event data recorders. The Committee also received briefings on using biometrics to identify people and measures to protect the privacy of certain personal information in court records.

As part of its study, the Committee discussed several bills referred to JCOTS by the House Committee on Science and Technology during the 2004 Session. The Committee discussed House Bill No. 1304 (Patron – Lingamfelter) on balancing civil liberties and law enforcement's use of potentially invasive technologies; House Bill No. 697 (Patron – Morgan) on event data recorders; House Bill No. 753 (Patron - May) on the misuse of social security numbers; and House Bill No. 543 (Patron - May) on limiting the use of unique identifying numbers in public records. The Committee also discussed proposals to create a FOIA exemption for unique identifying numbers; eliminate social security numbers from new land records; restrict personal identification information that can be required as a condition of accepting a negotiable instrument; and require state agencies and businesses to disclose breaches of databases to any resident of the Commonwealth whose unencrypted personal information may have been acquired by an unauthorized person.

The Committee adopted three recommendations. The first recommendation, based on HB 753, would prohibit making the social security number available to the general public and printing the number on an identification card. The proposal also would remove the number from state employees' insurance identification cards and prohibit suppliers from using the social security number when a consumer requests that his driver's license number be used. The second recommendation adopts the court clerks' request to extend by two years the sunset on their posting restrictions as set out in § 2.2-3808.2. The third recommendation adopts DMV's request for a study on the use of biometrics for identification.

With little change, JCOTS adopted the first two recommendations. Because JCOTS does not need a resolution to conduct a study, it declined to adopt the third recommendation and instead, agreed to include a biometrics study its 2005-2006 work plan.

Finally, JCOTS discussed and adopted a legislative proposal that would require manufacturers and lessors of motor vehicles that contain devices that record performance or operation information to provide notice of such devices to purchasers and lessees.

TABLE OF CONTENTS

REPORT OF THE JOINT COMMISSION ON TECHNOLOGY AND SCIENCE
to
The Governor and
The General Assembly of Virginia
Richmond, Virginia
May 2005

I. THE JOINT COMMISSION ON TECHNOLOGY AND SCIENCE (JCOTS)

To continue the work begun by the Task Force on Science and Technology established under House Joint Resolution 390 (1993), the 1996 General Assembly adopted House Joint Resolution 195, which created a joint legislative subcommittee to study science and technology. The subcommittee reported to the Governor and the 1997 General Assembly in House Document No. 81 (1997). The creation of the Joint Commission on Technology and Science ("JCOTS" or "Commission") was included among the recommendations of the subcommittee. Created by the 1997 General Assembly through House Bill 2138, JCOTS is a permanent legislative commission charged to study all aspects of technology and science, to promote the development of technology and science in the Commonwealth of Virginia through sound public policies, and to report its findings annually to the Governor and the General Assembly. (*See* Chapter 11 of Title 30 of the Code of Virginia, § 30-85 et seq.) JCOTS consists of seven members of the House of Delegates and five members of the Senate. JCOTS maintains a website at http://jcots.state.va.us/.

At its meeting on May 26, 2004, JCOTS adopted its 2004-2005 work plan (s*ee* Appendix 1). The work plan identified four issues for study through the work of advisory committees co-chaired by JCOTS members: Computer Crimes, Integrated Government, Nanotechnology, and Privacy. The work plan also identified new issues to be introduced at Commission meetings through testimony and presentations -- computer forensics and computer security -- as well as other issues to be monitored throughout the year, including privacy of personal information in court documents, taxes on Internet sales, and biometrics on identity cards.

To accomplish these objectives and establish its legislative agenda, JCOTS met four times from June 2004 to December 2004. During the period from June to November 2004, JCOTS' four advisory committees held 14 meetings (s*ee* Appendix 2). Approximately 72 people participated in JCOTS' work through membership on advisory committees (s*ee* Appendix 3). JCOTS received and adopted advisory committee reports and finalized its legislative recommendations for the 2005 Session its meeting on December 1, 2004.

II. JCOTS MEETINGS AND ACTIVITIES

A. ORGANIZATIONAL MEETING

The Joint Commission on Technology and Science (JCOTS) held its first meeting of the 2004-2005 interim on June 26. Commission members voted unanimously to re-elect Delegate May as chairman and Senator Stephen Newman as vice-chairman.

Chief Information Officer's Report on VITA

Lem Stewart, Chief Information Officer of the Commonwealth, briefed the Commission on the Virginia Information Technologies Agency's (VITA) progress since the agency's July 2003 creation. Mr. Stewart identified Virginia's two technology imperatives -- to establish Virginia as a leader in the use and management of technology in government, and to transition Virginia from a decentralized environment marked by stovepipes to a single IT "utility" that is highly effective, consolidated, centralized and headed by an enterprise CIO.

To realize these imperatives, VITA has several long-term goals. The agency wishes to ingrain the "build once, use many times" approach to service improvement to create a more efficient and consistent system. VITA also hopes to continually demonstrate improved service and savings benefits for citizens, customers, and taxpayers. Additionally, VITA is working to achieve true "transparency" as the state's IT utility. Another major goal is for VITA to become a catalyst for customer-centric state business transformations by supporting and encouraging business process reengineering, horizontally across state government, and vertically among other levels of government. VITA hopes to become a model of IT excellence in government.

Mr. Stewart described VITA's evolution in three stages -- formation, integration, and transformation. Formation occurred last year with the initial creation of VITA's structure and function and the formation of its enterprise governance model. Integration is currently in progress as the agency integrates the IT assets and staff from 90 agencies with minimal disruption of services. The third and final stage, transformation, is set to occur at the start of 2005, when VITA should meet its statutory requirement to take responsibility for all of the Commonwealth's IT resources and transform the IT environment in the Commonwealth.

Mr. Stewart shared the details of the ongoing integration stage. Over the course of this stage, VITA will be responsible for supporting 90 organizations at 1,497 locations, 60,000+ end users, 3,000+ servers, 12,500+ telecommunications devices, and 1,150+ employees. An integration of this magnitude presents many challenges. For instance, 90 percent of resources and infrastructure transition to VITA during the last six months of the integration. Additionally, VITA adopted a self-funding strategy, marking a significant departure from the previous general fund appropriation funding method. The agency also is attempting to show early savings, while concurrently trying to build a "mature" organization in 18 months. The challenges are not just abstract: VITA is working to implement significant change to outdated or non-existent administrative systems. Some of the systems in question are 20 to 30 years old. Finally, all of these efforts could be slowed by the human tendency to resist change.

Turning to the transformation stage, Mr. Stewart shared several items from VITA's business plan. The agency plans to start four initiatives in the fourth quarter of 2005: create a secure intranet, implement desktop management, implement statewide e-mail, and establish a customer care center. VITA also anticipates commencing a server consolidation at the start of 2005 and a data center for consolidated back up at the start of 2006.

Concluding his remarks, Mr. Stewart provided an update on VITA's progress in project management. VITA's enabling legislation places an emphasis on project management. Mr. Stewart reported that VITA has a project manager development program in place, through which 569 project managers and sponsors have completed overview training, 23 of these people are now "qualified" as project managers for major projects and 31 are now "qualified" as project managers for non-major projects. Mr. Stewart also summarized the present status of VITA's various projects. Of the 38 major projects on VITA's "Dashboard, " 21 are green, 3 are yellow, 0 are red, and 8 are in process. Together, these projects represent $961 million in total project costs. The agency also currently has 169 non-major projects submitted for review during fiscal year 2004, representing $70 million in total project costs.

Mr. Stewart concluded his presentation by telling the Commission that it can assist VITA by educating policy makers, employees and others that everything can not be done at once and must be done in phases; helping to overcome resistance to change; promoting an enterprise focus; supporting public/private partnerships; assisting in achieving consensus on expected results; and sharing ideas, suggestions, and expert guidance.

Information Technology Investment Board Membership

Section 2.2-2457 of the Code of Virginia establishes the Information Technology Investment Board (ITIB) and its membership. All appointed members must be non-legislators and citizens of the Commonwealth with experience in information technology systems or other technology systems. The Secretary of Technology and Auditor of Public Accounts serve on the Board as ex officio members. All members, except the Auditor of Public Accounts, can vote.

In 2003, the Joint Rules Committee appointed four members from a list recommended by JCOTS. The term of one such member, Hiram Johnson, was scheduled to end on June 30, 2004. The Commission discussed the matter, and voted to recommend Hiram Johnson to the Joint Rules Committee for re-appointment. The Joint Rules Committee subsequently approved his nomination, and his term will expire in 2008.

2004-2005 Work Plan

To conclude the meeting, staff presented a proposed 2004-2005 Work Plan. The Work Plan identified four topics for advisory committees to study: computer crimes, integrated government, privacy, and nanotechnology. JCOTS unanimously adopted the Work Plan. Delegate May announced that Senators Newman and Stolle and Delegate Rust will co-chair the Computer Crimes Advisory Committee, Delegates Nixon and Plum and Senator Howell will co-chair the Integrated Government Advisory Committee, Delegates May and Alexander and Senator

Watkins will co-chair the Privacy Advisory Committee, and Delegates Purkey and Cosgrove and Senator Wamplerwill co-chair the Nanotechnology Advisory Committee.

The Work Plan also identified topics to study through Commission meetings, including securing databases and personal computers. Continuing its tours around the Commonwealth, the Commission planned to tour the science and technology assets located in Virginia Tech and the Blacksburg area.

B. SCIENCE AND TECHNOLOGY AROUND THE COMMONWEALTH - BLACKSBURG

On Tuesday, August 3, 2004, the members and staff of the Joint Commission on Technology and Science toured facilities at Virginia Polytechnic Institute and State University (Virginia Tech) to learn more about the new technologies and applications currently being researched and developed.

System X - High Performance Supercomputing

Virginia Tech transformed the field of high performance supercomputer and garnered international prestige, winning top honors in Computerworld's international science category in June of 2004. Virginia Tech was cited for creating the fastest machine at any university in the world, and third fastest anywhere in the world, at a price of only $5.2 million; traditionally, such a machine would cost between $100 million and $250 million. Researchers built the supercomputer by connecting 1,100 Apple G5 computers to achieve a speed of more than 10 teraflops.

Virginia Bioinformatics Institute (VBI)

The Virginia Bioinformatics Institute's (VBI) research portfolio encompasses more than $40 million in grants and contracts since its creation in July of 2000. VBI serves as the genomics and bioinformatics core for a 15-university biodefense collaboration. Its most recent grant in excess of $10 million from the National Institutes of Health includes faculty from Virginia Tech's College of Engineering and the Virginia-Maryland Regional College of Veterinary Medicine. Among its projects is the Global Pathogen Web Portal Project (PathPort), a system that will enable researchers from around the world to collect and analyze data on pathogens that is stored in systems around the world. This tool will give them the ability to build upon one another's work and advance research to combat some of the deadliest pathogens in the world.

Nanotechnology: Cutting Edge Research Investment in Emerging Technologies

The Fiber & Electro-Optics Research Center (FEORC) in the College of Engineering has a long and distinguished record of extraordinary achievement in research and commercial development. The new Virginia Tech Applied Biosciences Center (VTabc), a University Center, shares facilities and personnel with FEORC and collaborates closely with it on nanotechnology research and commercialization. Created in 1985, FEORC's mission is research in advanced materials and electronics with emphasis in optics and sensors. Its researchers have engaged in more than 450 separate research programs, producing more than 1000 papers and more than 100 issued

patents. Eighty percent of its intellectual property is licensed by industry and it has spun off about 20 companies. VTabc conducts focused research and engineering activities involving optics and other disciplines to create knowledge and technology to benefit the medical, biomedical and veterinary fields, while supporting the practical goals of improving services and reducing the costs of health care. Among its projects are biocompatible coatings for implant structures, a revolutionary and inexpensive method for DNA analysis, and a targeted cell killing method that will someday replace chemotherapy. VTabc's efforts have led to commercialization successes that are five times larger than the U.S. university average per $1 million invested.

Unmanned Systems: A Market Drive Technology

Virginia Tech has developed internationally recognized unmanned systems programs with broad expertise and capabilities on the ground, under water, in the air, and even in space. The University's Center for Unmanned Vehicles simultaneously addresses the research and development needs of unmanned vehicle systems across autonomous air, land, sea and space systems. Some of these vehicles operate by remote control while others are self-powered and controlled. In addition to seeing pictures and videos of its systems, JCOTS members and staff witnessed the operation of self-powered and remotely controlled robots.

Virginia Tech entered the DAPRA Grand Challenge, a cross-country autonomous vehicle race from Los Angeles to Las Vegas. Out of 106 teams that entered, 25 were invited to qualify and 15 actually qualified. Seven teams completed the 1.35-mile qualification course, and only three universities' teams completed. Virginia Tech finished as the fifth seed overall. Next year, the prize doubles to $2 million. Virginia Tech also entered the 12th Annual Intelligent Ground Vehicle Competition. Twenty-eight university teams entered. Out of three separate challenges with first, second and third place awards, Virginia Tech won two awards in each challenge finishing first in two of them.

Unlike typical research programs, these programs primarily involve undergraduate students, although they often include graduate students as well. These programs serve as a test bed for unmanned systems research nationally and globally.

Virginia Tech Research Highlights

Dr. Charles Steger, Virginia Tech's President, explained other research initiatives taking place at the universityin transportation, power electronics, biomedical engineering, molecular medicine, and agricultural, and environmental issues. Built in collaboration with the Virginia Department of Transportation, Virginia Tech is home to the nation's only fully operational test road that can simulate most weather and lighting conditions encountered on the nation's highways. Its Center for Power Electronics Systems, a five-university consortium focused on efficient use of electrical energy, is one of the nation's few National Science Foundation Engineering Research Centers. In collaboration with Wake Forest University's School of Medicine, it developed the School of Biomedical Engineering & Sciences where researchers specialize in biomechanics, cellular transport, computational modeling, ergonomics, tissue engineering and much more. The University's Center for Molecular Medicine and Infectious Diseases researches the molecular events leading to immunological diseases and develops diagnostic tests and immunizations. The

Agricultural Research and Extension Centers develop new technologies to serve Virginia's agricultural, forestry, and seafood industries. Other research includes energy fuel, flexible solar cells and much more.

C. COMPUTER SECURITY

On Wednesday, September 8, 2004, the Joint Commission on Technology and Science (JCOTS) held a meeting to explore issues related to computer forensics and computer security. With a growing focus on protecting information and computer systems, JCOTS heard presentations on national and statewide efforts in this area. Presenters explained the vulnerability of computer information and the need for valid information security policies.

Computer Forensics on the National Stage

Supervisory Special Agent Christ M. Kacoyannakis, Assistant Director, Regional Computer Forensics Laboratory Program, Federal Bureau of Investigation, discussed the FBI's national initiative to provide forensic analysis and assist state and local law enforcement. He also provided an overview as to what information can be recovered and how they do it.

A Regional Computer Forensic Laboratory (RCFL) is a full service forensic laboratory devoted entirely to the examination of computer evidence in support of criminal investigations. Agent Kacoyannakis explained that the a unique law enforcement partnership promotes quality and strengthens computer forensics laboratory capacity. For the communities that they serve, RCFLs can be used to conduct forensic exams on all types of digital evidence, assist on searches, and train law enforcement. While they do not conduct investigations, the RCFL examiners provide technical advice and assistance to analyze computer evidence and provide expert testimony in court. To maintain impartiality, the examiners process, but never interpret, the data.

The first RCFL opened in San Diego in 2000. Today, there are nine existing labs with four more expected to be fully operational in 2005. The RCFLs handle thousands of cases and hundreds of terabytes of data every year. In 2003 alone, the RCFLs processed 82.3 Terabytes of data, accepted 1393 requests for service, participated in 196 search and seizure operations, trained 1525 law enforcement personnel, conducted 987 computer forensic examinations, and served 924 law enforcement agencies in five states.

The governance structure consists of three organizations. The National Steering Committee represents key stakeholder groups and advises on overarching policy issues. The Technical Review Board represents the computer forensic technical community and helps set technical operating standards. The Local Executive Boards represent the local participating agencies for each RCFL and provide operational guidance and oversight.

Each RCFL costs approximately $2 million to create, and $1 million annually to operate. Participating agencies receive computer forensic services and standards, capability, training, knowledge, and experience. Examiners gain access to training, networking, knowledge, and experience. Communities get high-quality service, crisis response capability, quality law enforcement, and national leadership. Currently, the RCFL Program is exploring improving

efficiency through technology by adding Storage Area Networks, expanding examination services, introducing PDAs, adding network forensics, and enhancing audio/video capabilities.

In addition to explaining the composition of the RCFLS, Agent Kacoyannakis also illustrated the role of the RCFLs and the examiners. For investigations of crimes against children, examiners lock a suspect's hard drive and retrieve active graphics files for use in prosecutions. They are able to retrieve these files even if the suspect has deleted them, because when a person deletes a file in a Windows system, the data contained in the file does not change or go away. The computer understands that the place where the data for this file resides may be reused, if needed, but is not overwritten. When investigators search hard drives, they retrieve these files in addition to any active files on the system.

Examiners can also retrieve documents when the system has been damaged. In one case, when the FBI announced that they were executing a search warrant at the home of a suspected child pornographer, the suspect dropped his laptop computer into the bathtub. Examiners were able to drain the water from the laptop and recovered all data from the hard drive. In another case, during the FBI's investigation of a child predator, investigators recovered several floppy disks from a motel room occupied by a female minor who had traveled from Chicago to Indiana to meet with a man she met on the Internet. She used a pen to punch holes through the floppy disk media. The FBI took the floppy disks apart, super glued the torn media, ironed the disk, and recovered most of the data from the floppy. However, not all data can be recovered. For example, examiners could not recover data from a hard drive that that had been shot by a 12-guage shotgun.

Computer Forensics in Virginia

First Sergeant Robert Keeton and Computer Forensic Examiner Christine Bryce, Computer Evidence Recovery Unit (CERU), Virginia State Police (VSP), discussed the responsibilities and activities of the CERU. Housed within the VSP, the CERU is the Commonwealth's computer forensics lab.

Sergeant Keeton explained that CERU examiners perform forensics exams, analyze information, and testify. Its caseload has grown so much that it completed more cases in the first nine months of 2004 than it completed in all of 2003. Sixty percent of the exams are for agencies other than the VSP, such as local agencies. A CERU costs approximately $50,000 to start and $20,000 - $30,000 for annual training.

After Sergeant Keeton's introduction, Ms. Bryce reviewed computer crimes laws in Virginia and the types of evidence hidden in various devices. Any digital or electronic device that uses or stores data has the potential to be evidentiary. Even if a suspect has "deleted everything," relevant data is still recoverable.

Information Security Policies

Steve R. Hutchens, Global Leader, Homeland Security, EDS, discussed the need for an information security policy and the elements it must cover.

Mr. Hutchens began by discussing threats and vulnerabilities. Threats are possible dangers to computer systems and include both active threats, which compromise authenticity, and passive threats, which compromise confidentiality. Vulnerabilities are weaknesses in computer systems that may be exploited to violate system security. Vulnerabilities include a failure to engage a firewall, incorrect configuration, undocumented features, errors in software that permit access, and functions that are used for purposes other than intended.

An adequate information security policy should minimize threats and vulnerabilities. It should include all resources -- people, technology, and operations -- and everyone in the organization must support and adhere to the security policy. The organization should limit access to information based on job functions and the need to know. Access limits should involve identification and authentication procedures that verify identity and ensure authority to access. The organization should also enforce password management that eliminates easy-to-guess passwords and requires changing passwords on an appropriate timetable. Organizations must stop the practice of using default passwords; websites list them and update them daily. Organizations also can use biometrics, smartcards, digital certificates, and access controls (i.e., controlling the ability to read, write, and run applications).

Technological resources must also support the security policy. This includes up-to-date virus protection software, firewall systems technology, intrusion detection, encryption, and network devices such as routers and switches. All of this technology, if properly used and regularly updated, can limit exposure to malicious software and intruders.

Operational resources initiate adequate operations procedures that everyone knows and follows. Organizations must plan and test disaster recovery systems, conduct security awareness training, and implement best practices for security management. They also must ensure regular and consistent system maintenance, including updating patches, virus signatures, and firewall technologies. Part of this maintenance will involve implementing a regular technology refresh cycle to ensure that security technology is up-to-date and that systems can handle new software.

Policy guidelines can come from a number of sources, such as the National Institute of Standards and Technology, industry groups, the SANS Institute – (SysAdmin, Audit, Network, Security), the National Security Agency for government systems, or be department or agency specific. An effective policy must support the organizational goals and objectives. It also must support the controls necessary to organizational integrity: management controls (for risks), operational controls (for people and procedures), and technical controls (for systems). Furthermore, the policy may address duties of loyalty, conflicts of interest, duties of care, privileges, accountability and management objectives.

A good policy will protect confidential information, establish “what is expected” of employees, and establish rights and privileges. It should guard against computer misuse and protect the organization from compliance issues (e.g., the Health Insurance Portability and Accountability Act (HIPAA) of 1996; the Federal Information Security Management Act of 2002 (FISMA); the Gramm-Leach-Bliley Act of 1999; the Computer Fraud and Abuse Act; the Federal Privacy Act

of 1974; the European Union Principles on Privacy; the Computer Security Act of 1987; the Security and Freedom Through Encryption Act; and the Economic Espionage Act of 1996).

Mr. Hutchens explained that in many cases, vulnerabilities and threats are inadvertently discovered by employees. Employees need to know to whom to report such discoveries. Without an audit and without employee participation, an organization will not catch insiders or outsiders posting pornography, music, or movies on corporate web servers, a definite liability issue. For those with the keys to the entire network, systems administrators, he recommends criminal background checks.

Computer Security in Virginia

Jerry Simonoff, Director of Strategic Management Services, and Jeff Deason, Director of Security Services, both with the Virginia Information Technologies Agency (VITA), discussed their agency's initiatives for the Commonwealth. VITA is the agency responsible for ensuring the security of state government databases and data communications from unauthorized uses, intrusions or other security threats. Section 2.2-2009 of the Code of Virginia requires the CIO to direct the development of policies, procedures and standards for assessing security risks, determining the appropriate security measures and performing security audits of government databases and data communications.

The Commonwealth of Virginia Strategic Plan for Technology assigns VITA four tasks for developing a statewide information technology security plan: design, develop, and implement a statewide security program and associated services; create a statewide information security office to include a cyber-incident response team and an IT security audit function; involve higher education in the statewide security program; and develop evaluation tools for measuring cost savings.

Today's computing environment is dependent upon vulnerable computer systems. The Commonwealth's systems rely on systems that control emergency response, the power grid, traffic controls, dam controls, and train switching. These systems contain and update criminal records and medical information. They also handle paychecks, social security and welfare checks, stocks, money transfers, Federal Reserve transfers, and international wire transfers. All of these critical systems face numerous threats from both inside and outside the organization.

A successful attack or compromising a system could lead to a failure to comply with regulations, loss of public confidence, theft of sensitive information, financial fraud, liability issues, sabotage, espionage, or malicious mischief. Whether the action is intentional (e.g., malicious code, hacking, or a prank) or unintentional (e.g., error), natural (e.g., flood or power outage) or manmade (e.g., a bomb), the resulting damage can be the same.

VITA's security planning follows two basic principles. First, the Commonwealth must protect the confidentiality, integrity, and availability of information systems. Second, security should be treated as a critical enabler. As the Commonwealth builds more enterprise systems and works with more partners, it has the opportunity to develop a statewide security system. However, this

carries with it a risk with increased exposure to systems over which it has no control. Because security is so critical, VITA will rely multiple solutions, instead of just focusing on one.

By mid-April 2005, VITA plans to complete an enterprise security risk assessment. By mid-year 2005, VITA expects to have a complete system in place. Such a system will include standards, policies and procedures; secure infrastructure and technical support; critical infrastructure and business continuity planning; risk management; information security training and awareness; and incident management. It will deploy all new systems in parallel to support the overall program.

As requested by JCOTS, VITA indicated it would report attacks on the Commonwealth's systems to JCOTS to make it aware of the level of threats as a way of informing the legislature when relevant.

Biometrics Technologies

Katherine M. Hollis, Director Security and Privacy Professional Services, EDS, demonstrated examples of biometric technologies that can control access to physical and digital infrastructures.

Biometrics are computerized methods of recognizing people based on physical or behavioral characteristics. The main biometric technologies include facial, fingerprint, hand geometry, iris, palm, signature, and voice recognition. Biometric technologies can work on a one-to-one level to authenticate a user, or on a one-to-many level to identify a user. However, only face, finger, and iris biometrics are capable of making a one-to-many identification.

For authentication, the system verifies the claimed identity of the user by comparing his biometric sample with one specific reference template, which is either physically presented by the user (e.g., a smart card) or pointed to in a database. For identification, the system identifies the end user from his biometric sample by associating it with his particular reference template based on a database search among the reference templates of the entire enrolled population.

Ms. Hollis demonstrated fingerprint-based technology using a one-to-one match. After registering a fingerprint with the system and recording it on a card, a subject inserted the card into a fingerprint reader. The subject then placed her finger on a scanner attached to an entry point (in this case, it was a small door). If they match, the subject gains access, and if they do not, the subject's access is blocked. With both one-to-one and one-to-many methods, the original fingerprints themselves are not stored anywhere on a network or computer system that an intruder might access. When a fingerprint is scanned, the characteristic points on the image are extracted and turned into a template. Only a digital representation of the specific points is stored, not the image itself. Because the template only holds information about points located on your fingerprint, the original image cannot be restored.

This technology is most commonly used for providing basic security such as entry to homes, and non-critical computers and information. However, the technology is not fool-proof. For example, a burned or severely cut finger can affect the system's ability to make a match, as can changes in skin elasticity caused by age.

D. YEAR IN REVIEW: FINAL MEETING

The Joint Commission on Technology and Science (JCOTS) held its final meeting of 2004 on December 1 to receive reports from the Secretary of Technology, the Chief Information Officer, and the President of the Center for Innovative Technology; to receive updates from the advisory committees; and to finalize JCOTS's legislative agenda for the 2005 Session. (*see* Appendix 4 for text of JCOTS recommended legislation, as introduced).

Secretary of Technology

Eugene Huang, Secretary of Technology, discussed his vision for the coming legislative session and the final year of the current administration. He explained that in his first two months as Secretary, he has been articulating a vision for technology in the Commonwealth that includes continuity of operations and outreach to stakeholder groups. Recently, he delivered the keynote speech to the Southern Piedmont Technology Council in Danville at the new Institute for Advanced Learning and Research. He said that what he saw was awe inspiring in how the Commonwealth is positioning itself to meet the global challenges of the twenty-first century.

Secretary Huang discussed his office's annual report entitled "Technology and Strategy Development in the Commonwealth." This report outlines the vision and agenda for the Office of the Secretary of Technology. The report fulfills two requirements contained within the Code of Virginia. The first is a requirement to deliver a biennial report on technology strategy as related to research and development goals for industry, academia and government in the Commonwealth. The second is a requirement to deliver an annual report on broadband communications services, high-speed data services and Internet access throughout the Commonwealth and future deployment potential of these services.

The report articulates a picture of technology in the Commonwealth today, and the challenges it faces in a global 21st century information-age society driven by technology. It contains four key sections: (i) research and development priorities, focusing investment opportunities in biotechnology, nanotechnology and defense and homeland security; (ii) broadband communications services; (iii) return on innovation and the efforts of the Center for Innovative Technology; and (iv) information technology reform and the efforts of the Virginia Information Technologies Agency (VITA).

Secretary Huang recognized that much of the focus to date has been on IT reform efforts and the establishment of VITA. While he stressed his commitment to ensuring the success of the IT reform effort, he noted that the report focuses on positioning the Commonwealth as a continued leader in not only the application of technology to the business of government, but also in fostering the development of technology industries as well.

Chief Information Officer

Lemuel Stewart, CIO of the Commonwealth, reported on the use and application of information technology by state agencies and public institutions of higher education to increase economic efficiency, citizen convenience, and public access to state government, as required by § 2.2-2007 of the Code of Virginia.

Without VITA, the Commonwealth would spend at least $1.1 billion over the next decade in duplicative, stand-alone administrative systems. The Commonwealth would likely see major project failures in excess of $120 million over the next six years. Aging systems with minimal security would continue to deteriorate and require more people and dollars for support. Infrastructure costs would increase, resulting in fewer dollars for citizen services and applications. The Commonwealth would not be able to provide citizen-centric, event-oriented services. Finally, the Commonwealth would be at a severe competitive disadvantage to other states.

To highlight the role of VITA in the Commonwealth, he listed the agency's accomplishments to date. It has successfully transitioned 90 executive branch agencies. It improved governance and oversight of technology investments by creating a Project Manager Development Program, instituting centralized procurement, and implementing an independent verification and validation program for all major projects. Through its procurement reforms, VITA has increased opportunities for small, women- and minority-owned (SWAM) businesses. It also has implemented standard compliance for security and software licensing. VITA has developed initiatives to self-fund cost of integration activities, expected to be approximately $6.7 million.

According to audited estimates, the Commonwealth with save more than $160.5 million over the next six years with $16.5 million and $26,125 million for the previous and current fiscal years, respectively. In addition, the agency completed a 26-item action plan created in response to the Auditor of Public Accounts' Special Report of December 15, 2003 and an employee classification study.

Looking forward, VITA has undertaken a number of major reengineering initiatives, including state-of-the-art data centers with disaster backup, an enterprise messaging and e-mail system, electronic government and associated business transformation, comprehensive statewide network services, and replacement of the Commonwealth's central administrative systems. Priorities for the year ahead include exploring public-private partnerships to transform the Commonwealth's IT infrastructure, instilling collaboration among all levels of government, expanding services to accommodate a mobile citizen population, recapitalizing IT in government, and encouraging strategic IT investment management.

Mr. Stewart concluded by illustrating and reiterating VITA's value to the Commonwealth. For its executive and legislative leaders, VITA offers the ability to better understand and manage the Commonwealth's IT investments and generate savings to reinvest in future technology projects. For the Commonwealth's IT employees, VITA offers the opportunity to learn new technologies, gain new skills, and advance in their careers. For the IT users, VITA offers the commitment to business continuity in the near term and better services over the long term. Finally, for the

Commonwealth's citizens, VITA offers the opportunity to interact with government in new ways, and the knowledge that the Commonwealth is investing hard-earned tax dollars wisely.

Center for Innovative Technology (CIT)

Peter Jobse, President of the Center for Innovative Technology (CIT), reported on the Center's initiatives and projects, its work plan for the year, and an overview of the results that it has achieved to date.

For 2004, CIT generated an economic impact of $230.2 million, nearly 25 percent more than its target of $185 million. This impact includes $49.9 million in small business in Small Business Innovation Research, Small Business Technology Transfer, and Advanced Technology Program awards and resulting sales and employment gains, $20.9 million in private capital raised and resulting sales and employment gains, $153.5 million in other revenue and employment growth, and $2.8 million in community broadband assistance.

Its 2005 operating plan includes four major goals. First, seeing a need to secure a nanotechnology specialization and an opportunity to define a biotechnology specialization, CIT plans to create new nanotechnology and biotechnology clusters. Second, observing an opportunity to increase defense related research, CIT and the Institute for Defense and Homeland Security will engage the public and private sectors to solve technological challenges through research and development. Third, in order to fill a significant void in angel and seed stage investment, reverse the reduction of technology start-ups in the pipeline, and meet a requirement to accelerate broadband deployment, CIT will strive to make the Commonwealth a leader in entrepreneurial ventures. Fourth, to meet its legislative support requirements, CIT will continue to support the Commonwealth's technology commissions. According to Mr. Jobse, CIT expects to have an economic impact to the Commonwealth of $119.4 million in 2005.

Joint Legislative Task Force and Joint Advisory Committee on Computer Crimes

JCOTS and the Virginia State Crime Commission combined their studies of the Computer Crimes Act and created a Joint Legislative Task Force and a Joint Advisory Committee. The Joint Advisory Committee on Computer Crimes was charged with examining the statutory basis for computer crimes and related laws in the Code of Virginia, including a determination of the appropriate definitions and elements constituting offenses, and recommending any necessary amendments in light of modern activities and technologies. The Joint Advisory Committee reported its recommendations to JCOTS.[1]

Computer crimes fall into one of three categories: the computer as a tool (e.g., used to commit fraud), the computer as the direct objective (e.g., theft of data), and the computer as the subject of the crime (e.g., spreading malicious code). While the offenses cover all categories, the vast majority fall into the "computer as a tool" category. All offenses in the Computer Crimes Act

[1] See Section III of this report for more detailed information on the work of the Advisory Committees during the 2004 Interim.

afford civil remedies to aggrieved parties and jurisdiction for the Office of the Attorney General. The Task Force and Advisory Committee identified nine specific threats: (i) phishing, spoofing, and disguising one's identity; (ii) bots and zombies; (iii) spyware and adware; (iv) viruses and worms; (v) falsifying certifications, seals, or other credentials; (vi) spam; (vii) identity theft; (viii) hacking and defacing websites, networks, and databases; and (ix) denial of service attacks.

Comfortable that the Code covers roughly half of the threats, the Task Force and Advisory Committee focused on the remainder. Between them, they recommended condensing and simplifying the definitions, basing many of them on those of the Uniform Computer Information Transactions Act. To protect against using non-computer devices with computer chips becoming computers under the Act, they voted to limit the coverage to general purpose, programmable computers. Most notably, the proposed bill requires that a person actually know or have reason to know that he was without authority, as opposed to merely acting without permission or right. Mitigating the impact of this final change, the crimes of computer fraud and personal trespass by computer would no longer require that a person take the underlying actions without authority.

To handle bots and zombies, the recommended legislation would add a provision to the computer trespass statute that criminalizes installing software without authorization. The bill also adds a subsection to address viruses and worms that do not harm computers, but hinder their ability to operate peripheral devices (e.g., grocery scanners, security cameras, and environmental sensors). In addition, the bill adds directly using a computer to obtain computer information without authority. To avoid criminalizing innocent or innocuous activities, the Task Force added a requirement that for an act to be actionable as Computer Trespass, a person must act with malicious intent. The proposal criminalizes using a computer with fraudulent intent to obtain, access or record identifying information, as defined by the identity theft statute (excluding name and birth date). Just trying to trick someone into revealing identifying information would be a crime; actually tricking them is not necessary. The proposal also specifically criminalizes using a computer to circumvent computer security measures. Finally, it clarifies that all property regardless of type can be stolen or embezzled.

Though JCOTS expressed concern over the number of new felonies created by the proposal, it adopted the proposal as drafted by a vote of four to one with one abstention.

Advisory Committee on Integrated Government

The Advisory Committee on Integrated Government was charged with exploring the issues created or enhanced by the transformation of government in the electronic age. The Committee continued focusing on the state of information technology (IT) procurement in the Commonwealth, and addressed competing provisions dictating electronic meetings requirements for public bodies.

The Committee voted to recommend for consideration four proposals introduced by VITA. The first would eliminate a preference in the Virginia Public Procurement Act for competitive sealed bidding over competitive negotiation. The second would allow public bodies to purchase information technology and telecommunications goods and services from online public auctions and through cooperative procurement arrangements with approval of the Chief Information

Officer. The third would authorize VITA to conduct an Alternative Dispute Resolution Pilot Project. The final would allow public bodies to hold closed meetings to discuss records already exempt from public disclosure relating to the Public-Private Education Facilities and Infrastructure Act (PPEA). Believing that procurement reforms beyond technology were outside its mandate, JCOTS declined to adopt VITA's other proposal that would eliminate the preference of competitive sealed bidding over competitive negotiation.

The Committee also recommended amendments to the electronic meetings provisions of the Virginia Freedom of Information Act (FOIA). A Pilot Project, established in 1999, provided an alternative from FOIA for certain meetings held via videoconference.[2] The Pilot Project will expire on July 1, 2005 absent legislative action. Working with a FOIA Council subcommittee, the Committee proposed reconciling the provisions in the Freedom of Information Act and the Acts of Assembly to create one set of requirements for electronic meetings. However, unlike the FOIA proposal, the Committee proposed retaining the current Acts of Assembly provisions that enable a quorum to be distributed across remote sites and do not require that remote sites be open to the public. In voting to recommend the bill, JCOTS conformed the electronic communications meetings bill to the FOIA Council proposal by retaining the current FOIA requirements for a physical quorum and remote sites open to the public. JCOTS also amended the bill to clarify that the General Assembly could not meet electronically during regular, special, or reconvened sessions.

Advisory Committee on Nanotechnology

The Advisory Committee on Nanotechnology was charged, pursuant to House Joint Resolution 120 (2004), to identify nanotechnology research and economic development opportunities for the Commonwealth and to consider the efficacy of creating a statewide, comprehensive and coordinated strategy to secure additional federal research and development funds and to boost commercial activity in this fast growing sector.

While the Committee made no formal legislative recommendations, it focused on three key areas: commercialization (bridging the gap between research and commercialization), education, and financing (including business development and incentives). The Committee agreed that the Commonwealth should establish a more permanent body to continue discussions about nanotechnology in the Commonwealth. Adopting this recommendation, JCOTS agreed to include nanotechnology in its 2005-2006 work plan.

Advisory Committee on Privacy

The Advisory Committee on Privacy was charged with (i) reviewing current privacy laws and practices as they pertain to information and (ii) proposing policies and guidelines for public bodies to evaluate the use of potentially invasive technologies when determining whether to support their use financially or to authorize or prohibit their use.

The Committee adopted three recommendations. The first recommendation, based on HB 753, would amend the Personal Information Privacy Act by restricting the use of social security

[2] Citation for pilot project

numbers. Among other things, the proposal would prohibit making the social security number available to the general public and printing the number on an identification card. The proposal also would (i) require that insurance plans for state employees assign an identification number that is not a covered employee's social security number and (ii) amend the Virginia Consumer Protection Act to prohibit a supplier from using a consumer's social security number when the consumer requests that his driver's license number be used.

The second recommendation adopted the court clerks' request to extend by two years the sunset on restrictions for posting court records on the Internet set out in § 2.2-3808.2. The third recommendation adopts DMV's request for a study on the use of biometrics for identification. With little change, JCOTS adopted the first two recommendations. Because JCOTS does not need a resolution to conduct a study, it declined to adopt the third recommendation and instead, agreed to include a biometrics study its 2005-2006 work plan.

Finally, JCOTS discussed and adopted a legislative proposal that would require manufacturers and lessors of motor vehicles that contain devices that record performance or operation information to provide notice of such devices to purchasers and lessees.

Discharge of the Advisory Committee Members

As the final order of business, Chairman May thanked and discharged the members of the advisory committees. He thanked everyone for their hard work and dedication to the science and technology issues facing the Commonwealth and expressed his hope that they would continue to serve the Commonwealth next year.

III. ADVISORY COMMITTEE REPORTS

JCOTS established four Advisory Committees to study various issues throughout the 2004 Interims, and make recommendations to JCOTS. Each of the Advisory Committees met throughout the interim, as detailed below.

A. COMPUTER CRIMES

- **Delegate May (JCOTS) and Delegate Albo (Virginia State Crime Commission), co-chairs**

In an effort to strengthen Virginia's computer trespass statute, House Bill 566 (Albo) and Senate Bill 275 (Devolites) were introduced during the 2004 Session of the General Assembly. The House Committee on Science and Technology referred these bills to JCOTS. In examining the bills and the existing language of the computer trespass statute, the House Committee on Science

and Technology (HCST) and the Senate Courts Committee had expressed concern that the bills and the entire Computer Crimes Act may inadvertently criminalize innocent conduct. The HCST carried over bills and asked the Joint Commission on Technology and Science (JCOTS) to study the issue. Recognizing that the entire Computer Crimes Act, originally enacted in 1984, needed to be revisited in light of evolving technology, JCOTS included a complete study in this year's work plan to review the Computer Crimes Act and related laws and to evaluate the need for special laws on computer-related conduct.

In addition to the JCOTS study, the 2004 Appropriation Act directed the Virginia State Crime Commission (VSCC) to "examine the statutory basis for computer crimes in the Code of Virginia, including a determination of the appropriate definitions and elements constituting offenses in this area." JCOTS and the VSCC combined their efforts and created a Joint Advisory Committee on Computer Crimes and a Joint Legislative Task Force to bring together technical and legal experts on the matter.

Computer Viruses and Malicious Code
House Bill No. 566 / Senate Bill No. 275

HB 566 and SB 275 were presented to the Advisory Committee to initiate discussion. While both bills were introduced in the same form with the same intent, they arrived at the HCST taking different approaches. HB 566 provided that adding or altering information without authority is computer trespass and elevated the crime to a Class 6 felony if certain aggravating factors are present. SB 275 created a separate crime providing that knowingly and maliciously inserting a computer virus into a computer, computer program, computer software, or computer network of another without the knowledge and permission of the owner is a Class 1 misdemeanor.

Members of the HCST had raised a number of concerns with the bills. On its face, HB 566 would criminalize innocent acts such as sitting at the wrong computer and updating the software or merely hitting one key. In addition, a person could violate the statute without even knowing that he lacks the authority to use the system. The statute is also unclear about whether the property that is damaged must be worth $2,500 or more for a violation to occur or the damage must be $2,500 or more. These issues exist even without the changes proposed by HB 566.

SB 275 attempted to address these concerns by creating a separate crime and defining a computer virus as "a computer program or other set of instructions that is designed to degrade the performance of, or to disable a computer or computer network and to have the ability to replicate itself on other computers or computer networks without authority of the owners of such computers or computer networks." The trouble with this definition is that is both overbroad and underinclusive. The statute could criminalize the legitimate use of software that disables computers, but not the use of viruses that do not replicate themselves, worms, trojan horses or other malicious code.

Charles Curran, Assistant General Counsel of America Online (AOL), explained that he approached Delegate Albo and Senator Devolites about introducing a bill to criminalize computer viruses. Last year, AOL changed its tactics from combating falsification to combating

those who take over other computers or conceal their identities to falsify information. Hackers and spammers are evading the current laws by using viruses and trojan horses to take over other computers and violate the law. Mr. Curran asked whether the current penalties and damages were sufficient to address these actions. Spammers have already shown that they would suffer millions of dollars in penalties and injunctions as a cost of doing business, so criminal penalties were needed. The problem reached a threshold that made criminal penalties necessary.

The Committee discussed a number of issues issues raised by these bills. The law needs to focus on the "bad actors," -- i.e., those who use a computer without authority with the intent to do something improper like infect a machine, download unsolicited code or distribute malicious code. The law must address those who use viruses to distribute code and those who have a secondary purpose such as notifying others of vulnerabilities or protected information. Unfortunately, creating a broad law with exemptions or a specific references to particular technology would likely become outdated before it even takes effect.

It was obseerved that to accomplish the goals of the Committee, HB 566 was too broad and SB 275 was too narrow. For example, the scob trojan was designed to reach a computer and send sensitive information to a third party, but it is not self-replicating. Arguably, HB 566 would treat it as a misdemeanor and SB 275 would not address it all. To further caution the Committee about how difficult drafting a statute would be, it was illustrated that criminalizing the downloading of software without permission would not only affect spyware, adware, keystroke loggers and "drive-by" downloads, but could also affect the use of cookies, a commonly accepted practice. Perhaps the true crime involves a financial motivation or the attempt to disguise one's identity to commit a crime.

The Virginia Computer Crimes Act

As the discussion continued, it turned toward the issue of prosecution and the need for high profile cases to make those who would violate the law think again. The prosecutors in the group explained that prosecutions in this area are labor-intensive, taking months or longer to investigate and bring to trial. Laws must be easier to prosecute to be effective. Prosecutors are not required to prosecute Class 1 misdemeanors and they are often not worth the time and energy. It was suggested to increase the penalty to a felony. Inconsistencies in existing law were also discussed. For example, while destruction of property requires damage in the amount $1,000 to be a felony, damage to computer information (computer trespass) requires $2,500 worth of damage.

Several members of the Committee and the audience focused on one point: customers want protection from the high-tech misdeeds of others. As one member put it, he wants to be protected from the denial of his resources, the use of his resources without permission and others who try to steal his personal information. In comparing the risk of computer crimes to that robbery, one committee member noted that there is an arguably low risk that a given person will commit robbery because it has a high penalty and is socially unacceptable. However, computer crimes bring a high risk because there are low penalties and in many cases, it is socially tolerable, if not acceptable.

The Committee was reminded that consumers and businesses were not defenseless in this area, noting that tools are available through the commercial market, including some available for free. He cautioned the Committee in its deliberations to not interfere with the transfer of legitimate communications, for example, by penalizing valid advertising models (e.g., requiring that customers view advertising in exchange for free e-mail) or burdening Internet conduits.

The Committee agreed that it should focus on the behavior. One recommendation was to identify threats, look at the Code of Virginia to determine if it is addressed and then define the action, if necessary. The Committee identified the following threats: (i) phishing, spoofing and disguising one's identity (faking an identity to gather personal information); (ii) bots and zombies (programs implanted into a computer that allow third parties to use it); (iii) spyware and adware (a category of software that, when installed on a computer, may send pop-up ads, redirect the browser to certain websites, monitor the websites visited, or even log each key hit); (iv) viruses (programs or pieces of code that are loaded onto a computer without the user's knowledge and run against his wishes; some viruses can replicate themselves) and worms (programs that propagate themselves across a network, using resources on one machine to attack other machines) (a virus can insert itself into other programs, a worm cannot); (v) falsifying certifications, seals or other credentials; (vi) spam (unsolicited bulk electronic mail); (vii) identity theft; (viii) hacking and defacing websites, networks and databases; and (ix) denial of service (DoS) attacks (an attacker attempts to prevent legitimate users from accessing information or services) and distributed denial-of-service (DDoS) attacks (an attacker uses others' computers to attack another computer).

Staff reviewed each threat in light of existing statutes. Falsifying seals, certifications and other electronic authentication credentials is prohibited by laws pertaining to unfair and deceptive trade practices, such as the Virginia Consumer Protection Act, trademark and copyright laws, and fraud laws. Some spam, known as unsolicited bulk electronic mail, is prohibited by section 18.2-152.3:1 of the Computer Crimes Act. Identity theft is prohibited under section 18.2-186.3, regardless of how the information was obtained. Phishing, spoofing, and disguising identity; bots and zombies; spyware and adware; and viruses and worms are partially addressed by fraud and identity theft laws. However, violations of those laws require someone to actually be injured, but by then, the harm is already done and the law is not much of a deterrent. The Committee believed that the attempt itself should be criminalized. To address those specific issues, staff drafted two legislative proposals.

Computer Invasion of Privacy Proposal

Current section 18.2-152.5 makes it a crime for any person to use a computer or computer network and intentionally examine without authority any employment, salary, credit or any other financial or personal information relating to any other person. Violations are punishable as a Class 1 misdemeanor. To strengthen this provision, it would be amended to replace "personal information" with "identifying information" as defined in the identity theft statute (subdivisions (iii) through (xiii) of section 18.2-186.3.C). This change was proposed to avoid criminalizing legitimate business practices while focusing those that involve gathering specific information that no legitimate business practice would involve gathering without authority. In addition, the penalty would increase to a Class 6 felony for repeat offenses and a Class 5 felony if the information is sold or used in another crime.

Because the Committee wanted to criminalize not only examining the information without authority, but also any attempt to gather it by deception, it discussed creating a new statute that would address phishing, spoofing, and other deceptive means of gathering information. Any person who used a computer or computer network with the intent to fraudulently obtain, record or access identifying information would be guilty of a Class 6 felony. Like violations of computer invasion of privacy, selling the information gathered in a violation of this section or using it another crime would be a Class 5 felony.

For the current statute, the Committee questioned whether an exemption for employers, law enforcement, and network security personnel was necessary. Chairman Albo apprised the Committee that while no other provision of the criminal code contains a specific law enforcement exemption, the common law and other general provisions of the criminal code address law enforcement. For employers, their authority to use and view information is governed by state and federal employment laws. To address issues of network security and verification of user license or authorization, staff agreed to draft an exemption for future discussion.

For the new statute, the Committee questioned whether requiring a fraudulent intent would require proof of intent to take something physical from a person. Convinced that the word "fraudulently" only required intent to deceive, it voted to use this standard.

Computer Contamination Proposal

The second proposal addressed viruses, worms, Trojan horses, and other malicious code by defining such programs as computer contaminants and making their use a Class 1 misdemeanor. Second convictions or engaging in six defined acts considered dangerous would raise the penalty to a Class 6 felony. The proposal defined a computer contaminant as any set of computer instructions that are designed to (1) alter, damage, destroy, or monitor information within a computer or network without the authorization of the owner of the information, (2) degrade the performance of or disable a program, computer or network without the authorization of the

owner, or (3) allow a person the ability to use or operate a computer or network, without the authorization of the owner.

The Committee was uncomfortable with defining a computer contaminant fearing that a definition would become obsolete. The task then focused on criminalizing use of malicious code or malicious programs that replicate without defining it specifically. The Committee opted for a more general provision that focused on a bad actor with a bad intent committing a bad act.

The Computer Crimes Act - Revised

Staff of the Virginia State Crime Commission and JCOTS reviewed the proposals with the Committee. To modernize the Code, staff proposed definitions that mimic those found in the Uniform Computer Information Transactions Act (UCITA). Broader definitions will hopefully avoid obsolescence problems facing the law in addressing technology. Some existing definitions would be removed or combined with others. Under the revisions, a computer is a computer, property is property and computer information is computer information regardless of the type or form. Finally, prosecutors must prove that a defendant knew or had reason to know that he was without authority.

"Computer Fraud" and "Personal Trespass by Computer" would no longer require proof that the computer use was without authority. It would not matter whether the person used a computer or network without authority so long as he took the underlying action without authority, knowing that he had no authority to do it.

The crime of "Computer Trespass" would be expanded to address denial of service attacks and defacing websites. After the Committee proposed eliminating the computer contaminants bill, staff redrafted the statute to address malicious code and the earlier issues that were raised. Elements of the new statute were "using a computer or computer network, directly or indirectly" (addressing automated software and remote controls), "with the intent to maliciously" (addressing the issue of knowledge and bad intent) take the actions specified in subdivisions 1-6. In addition to the prohibited actions, the proposal added damaging, destroying, disabling or monitoring computer information to the prohibited actions. Because the Task Force had voted to remove the malicious requirement and some of the underlying actions could be benign, a new subsection B was added to require that altering, monitoring or installing computer software or computer information be malicious to be a crime. The remaining provisions require that the act be intentional and without authority. In addition, the presence of specified aggravating factors makes the crime a felony. The amount of damage also was reduced to $1,000 to be consistent with other provisions in the Code.

The crime of "Computer Invasion of Privacy," which addresses in part identity theft, was clarified and strengthened. The proposal replaces "personal information" with "identifying information" as defined in the identity theft statute (minus name and birth date) and increases the penalty for subsequent violations, selling or distributing the information, or using the information to commit another crime. In addition, the provision would offer an exemption for network security. It would be a crime for someone to view information that could be used to access financial information or create identification without authority

To address phishing, spoofing, spyware, adware, bots, zombies, viruses and worms, falsifying seals and disguising identity or otherwise deceiving someone to gather information, the proposal would create a new crime of using a computer to gather identifying information. The provision would make it a criminal act to use a computer or computer network with the intent to deceive someone into providing information that no one has a legitimate reason for gathering by deception. The information is limited to identifying information as defined in the identity theft statute (minus name and birth date). The crime would be a Class 6 felony and would be elevated to a Class 5 felony if the perpetrator sold or distributed the information or used the information to commit another crime.

The Task Force talked about merging this section with the identity theft statute. However, the identity theft statute currently requires an additional intent to use the information, not just gather it. The computer crime only requires proof of the intent to gather it and offers a private right of action. The Committee determined that there exists no legitimate reason for engaging in these actions, and criminalizing the act of gathering the data would enable law enforcement and individuals to fight identity theft at an earlier stage.

To address bots, zombies, worms, viruses, cracking (also known as hacking), and other forms of computer and computer network invasion, the proposal created a second new crime of using a computer to gain unauthorized access. One subsection would prohibit using a computer or computer network with the intent of allowing someone the ability to gain future access. Another subsection would prohibit using a computer or computer network with the intent of actually invading a system. The crime would be a Class 1 misdemeanor, elevated to a Class 6 felony for second and subsequent offenses, violating the provisions in the commission of another crime, or gaining access to three or more computers or one or more computer networks. The Committee decided to merge the provisions into the "Computer Trespass" statute.

Finally, the proposal would expand the definition of property for all larceny crimes. Currently, most intangible personal property, including computer information and services, is considered property only for purposes of the embezzlement statute. However, if it is considered property capable of embezzlement and embezzlement is deemed larceny, it naturally follows that it should be considered property for the larceny statutes as well.

The Committee forwarded its work to the Joint Legislative Task Force and JCOTS for consideration.

B. INTEGRATED GOVERNMENT

- **Delegate Nixon, Delegate Plum, Senator Howell, co-chairs**

The Advisory Committee on Integrated Government met four times during the 2004 interim on June 30, August 17, October 5, and November 16. During its meetings, the committee received briefings on and discussed information technology (IT) reforms, the move toward interoperable communications, electronics recycling, electronic transactions, offshoring and using electronic communications to conduct meetings.

Virginia Information Technologies Agency
Project Management Division

Lem Stewart, Chief Information Officer of the Commonwealth, and Jerry Simonoff, VITA's Director of Strategic Management Services, briefed the Committee on VITA's Project Management Division. Prior to VITA's implementation, projects were not reviewed until they reached the procurement phase. VITA's predecessor agencies had the opportunity to review the project, but their ability to make any adjustments was limited. Now, VITA is instituting project management not only because it is a requirement, but also because it is the best practice.

Commonwealth Project Management (CPM) is the application of knowledge, skills, tools, and techniques to meet or exceed stakeholder needs and expectations from a Commonwealth Project. The objective of CPM is to define a structured, disciplined approach for project management in order to deliver anticipated benefits from business-driven IT investments. It focuses on the scope, costs, schedule, performance and risk of the project and encompasses the entire life cycle of the project from selection to closeout review.

The CPM project life cycle for major IT projects (based on costs and impact to the Commonwealth) involves the proponent agency, that agency's Secretariat, VITA's Project Management Division, the CIO and the ITIB. Each group plays a role as the agency seeks approval for project selection, initiation, planning, and implementation approval, as well as project closeout. Throughout the process, agencies must create an IT strategic plan, propose and justify projects, establish their purpose, develop detailed project plans, draft status reports and evaluations and conduct post implementation reviews. The Secretariat reviews the agency's work and resolves issues that may arise. VITA's Project Management Division also reviews the agency's work and assists and supports the agency throughout the process. The CIO approves the agency's strategic plan, recommends project initiation to the ITIB, resolves issues as needed, monitors the project and has the authority to modify, suspend or recommend termination of the project. Finally, the ITIB has the authority to approve the project initiation, and to terminate the project at any stage.

The CPM ensures that the process is value and outcomes driven, customer service focused, and transparent. The process also ensures stakeholder involvement and best practices. VITA guides the process through the development of project management policies, standards and guidelines. Project planning approval criteria includes the degree to which the project is consistent with the Commonwealth's overall strategic plan; the technical feasibility of the project; the benefits to the Commonwealth of the project, including customer service improvements; the risks associated with the project; continued funding requirements; and past performance by the agency on other projects. All major IT projects require independent verification and validation (IV&V) of project fulfillment is required during planning and execution. The IV&V strategy must be approved as part of the project development approval. The Project Management Division will implement a comprehensive IV&V program as a VITA service offering using VITA-qualified IV&V vendors. IV&V reports will supplement and validate dashboard reporting. VITA also requires a project closeout report, which measures outcomes, identifies lessons learned and identifies best practices.

Cabinet Secretaries, the CIO and the ITIB oversee project execution and control through "Dashboard Status Reporting." The Dashboard is a Web-based status reporting system that provides concise and timely summary status of major IT projects. It establishes a consistent, common framework for agencies, Secretariats, and the CIO to update project activity, monitor progress, and assess risks. It also enhances their ability to respond to project changes in a timely manner, increases accountability, improves project management capabilities and provides a public view on the VITA website.

As part of the process, VITA has established a project manager training and selection process. This process establishes a common minimum baseline of knowledge standards, and emphasizes the balance of training, experience, and knowledge. It is the first step in establishing a Commonwealth IT Project Management Community. This cost-effective program ensures an improved project management capability.

When asked how they avoid over-managing, Mr. Simonoff responded that VITA drafted a matrix based on the difficulty and complexity of the project to determine project management components necessary for a given project. VITA is attempting to relate the project management phases to other processes, such as IT resource and portfolio management. The agency is also implementing a "FedEx"-style tracking system for IT project approvals. It has also integrated the project management process with the PPEA process. The agency is developing a stakeholder-driven process focusing on specific projects and processes, while the ITIB is taking a broader look at the entire landscape of projects and future direction of the Commonwealth.

Public Private Partnerships

Mr. Stewart and Mr. Ziomek also briefed the Committee on proposals received under the Public-Private Education and Infrastructures Act (PPEA).

The Commonwealth does not have $400 million to invest in infrastructure and facilities. nor does it have the people, time, or resources to implement large-scale projects. Potential partners bring to the table innovative ideas for solving business problems, access to state-of-the-art capabilities and technologies, expertise and ability to bring major projects to completion, and the ability to bring resources to bear for the benefit of citizens and customers. The Commonwealth sets the parameters by defining what is and is not acceptable in proposals. The ultimate goal of the process is to selectively seek investment in those public-private partnerships that best serve the business-driven technology needs of the Commonwealth, and support the agency mission, vision, and objectives established in the VITA Business Plan.

Proposals can only be submitted for "qualifying projects," as defined in §56-575.1 of the Code of Virginia. Included among those projects are technology infrastructure projects. The proposal must serve a public need and purpose, the estimate cost must be reasonable in relation to similar projects, and the private partner's plans must result in the timely acquisition, design, and implementation of the project.

From November 2003 to March 2004, VITA received initial PPEA proposals. Then, the agency researched the PPEA legislation and model procedures, drafted the initial process model, and

established an enterprise projects office. Finally, in April 2004, VITA established its "Internal VITA PPEA Proposal Review Committee." The Committee conducted an initial review of the proposals, drafted the "Attributes for VITA PPEA Proposals," and established a contract for a high-level sourcing consultant. After that review and before VITA posted the proposals, "Attributes" and invitation for competing proposals, VITA met with proposal teams and allowed them to update their proposals.

The review committee makes its recommendation to the CIO, who determines whether the proposal is worth pursuing under the PPEA and makes recommendations to the Information Technology Investment Board (ITIB). If the project is accepted, the ITIB, with input from the Cabinet, will prioritize the project and include it in the annual report to the Governor and General Assembly. After the initial review, the Committee conducts a conceptual review by posting for competing proposals and evaluating all submitted proposals. The CIO accepts or rejects the proposals and makes a recommendation to the ITIB. If the ITIB approves the project, the Committee conducts a detailed review. If the CIO approves the project and proposal, he will recommend that the ITIB grant development approval. The last step is negotiating a comprehensive agreement, which the Attorney General reviews, the General Assembly decides whether to fund and the Governor decides whether to approve.

Five groups have proposed projects to VITA. Northrop-Grumman, Virginia Commonwealth Partners (headed by IBM), Virginia Business Modernization Initiative (headed by CGI-AMS) and Virginia First (headed Kroll and EDS) proposed data center construction and consolidation to provide enterprise-wide system support and back up. Gateway proposed a desktop modernization program to replace all desktop hardware and provide e-government development tools and training. All proposals, with the exception of the Gateway proposal, were accepted. The CIO rejected the Desktop Modernization proposal because of its narrow scope and existing sourcing options. Parts of the proposals that VITA initially received were on target, but none had the scope or balance that VITA anticipated. VITA made a concerted effort to publish its Business Plan to frame the planned transformation and published Attributes to broaden the scope of existing and future proposals. Mr. Ziomek highlighted that PPEA is not new, but an extension of the partnerships that already exist with Departments like TAX and Transportation. It is not business as usual.

PPEA proposals must be open to the entire Commonwealth and must include enterprise integration. Some proposals naturally lend themselves to local government involvement. When that happens, the proposal is subject to a local government review to determine the impact to local government. VITA is using PPEA and technology to "better the business."

Attributes for VITA PPEA Proposals

VITA is currently posting unsolicited proposals for competitive response. These proposals offer comprehensive solutions for the delivery of innovative technology and infrastructure projects through the establishment of partnerships under the provisions of the PPEA. VITA and its customer agencies are focused on making significant improvements in Commonwealth technology management that will deliver measurable business value and service to the citizens of Virginia and the customers of state government. It is considering PPEA partners to do the

"heavy lifting" associated with major Commonwealth business and technology transformation. Prospective partners must possess the demonstrated capability to manage and serve the technology needs of an organization the size and scope of the Commonwealth of Virginia. Companies interested in potential partnerships should consider the following guidance when preparing PPEA proposals. It is anticipated that proposals would provide comprehensive business and process solutions that address the majority of the "major reengineering initiatives" presently under consideration - (i) State-of-the-Art Data Center(s) with Disaster Backup, (ii) Enterprise Desktop Management, (iii) Enterprise Messaging/E-mail System, (iv) Enterprise Customer Care Center, (v) Electronic Government and Associated Business Transformation, (vi) Comprehensive Statewide Network Services, (vii) Enterprise Application Level Access Management (single sign on), (viii) End-to-end Systems and Process Management (organization, technology, process, facilities, and security), (ix) Continuous Evaluation and Planned Implementation of Emerging Technology (planned technology refreshment), (x) Change Management Processes, both Organizational and Technical, that Operationalize Technology, and (xi) Integrated Management of Distinct Transformation Projects and Activities (with separation of infrastructure and enterprise application initiatives, including separate cost justification). VITA remains free to select any or none of the proposals submitted.

Management Commitment: Proposals should demonstrate the credibility of the supplier's commitment to provide the proposed services. Proposals should define the management and organizational structure for effective ongoing conduct of the partnership with VITA, within the context of existing Commonwealth governance processes.

Understanding of Commonwealth Issues: Proposals should demonstrate the supplier's ability and willingness to: (i) propose terms that are appropriate to the environment in which VITA and its customer agencies operate; and (ii) provide maximum flexibility in terms of the services provided and the fees charged while adjusting to changes in the business requirements of the Commonwealth over the term of the agreement, and changes in technology. A Commonwealth priority is the support for community development and associated technology job growth in rural and economically depressed areas within the Commonwealth. Partnering with firms that have a strong presence in the Commonwealth, financially and numerically, is important.

Impact on Employees: Employees are our most valuable assets and the key to the success of any partnership. Proposals must take into consideration the importance of professional development, career advancement, challenging opportunities and minimize the impact on employees throughout the transformation process. .

Work Approach: VITA seeks a service level based approach that is customer and citizen-centric and clearly demonstrates the willingness to satisfy or exceed service level requirements. The quality of management, the technical approach used to assure consistently high quality service, and the willingness to advance concrete proposals on all pertinent matters, rather than deferring issues or deliverables to later stages or post-closing presentations or negotiations, must be demonstrated in the proposal.

Implementation/Transition: Commonwealth agencies would experience no loss of service or decrease in productivity throughout the transformation process. A phased project

implementation plan is essential, characteristic of a self-funded model. Suppliers must demonstrate commitment to a smooth partnership exit strategy in the event of program termination, including the provision of transition assistance.

Supplier Viability: Supplier's size, financial stability, industry track record, and capacity to provide the managerial, technical, and physical resources to deliver the proposed services over the required period must be demonstrated.

Experience in Providing Comparable Services: Supplier's specific experience and ability in providing the proposed services to entities on a scale and/or complexity comparable to the Commonwealth. Proposals should further demonstrate the professional qualifications and experience of assigned personnel including the assigned personnel's ability to perform the work as reflected by technical training and education, general experience and specific experience in providing the proposed services.

Financial Considerations: Detail the terms and fees for all proposed services, the degree of growth and inflation protection included in the baseline prices, the mechanism for adjusting pricing due to increased or decreased levels of proposed service, and transition, migration and termination considerations. Suppliers should provide an ongoing comparison of price to a theoretical Commonwealth managed effort to provide similar services (same resource costs and timelines), establishing the baseline against which the partnership will be evaluated.

Corporate Policies: Proposals must demonstrate the level, relevancy, and quality of participation by Small, Woman-owned and Minority-owned Businesses (SWAM). Proposals also should provide a corporate ethics policy and demonstrated practice of the policy.

Communication Plan: Proposals should define a Comprehensive Communications Plan to support proactive communications with all stakeholders.

Asset Retention/Ownership: A plan for, and supplier's expectations regarding, the ownership, retention, and use of assets (including intellectual property) used or developed in connection with the partnership, including from inception of such a partnership to dissolution, must be presented.

PowerPoint Presentation: Proposals should include an executive level PowerPoint presentation of the proposal.

Evaluation of Competing Proposals: Using the information from other proposals posted on the Commonwealth Web site for competition, suppliers should include a white paper analyzing and evaluating the strategy, advantages, disadvantages, value to the Commonwealth and its citizens, approach, etc. of its competitive submission, as compared to posted proposals.

Representative Transactions: All proposals should provide a documented reference library of successful (in terms of value and effectiveness) implementations conducted by the supplier in relation to US public-private partnerships providing services to citizenry

Compliance with VA Code: Suppliers must describe, in detail, how their proposals conform to the definition of a "Technology Infrastructure Project" as presented in §56-575.1 of the Code of Virginia and how it serves the public purpose described in §56-575.4(C) of the Code. Suppliers are reminded that their proposals must conform to the provisions of § 2.2-2012 A of the Code of Virginia relating to the information technology accessibility standards contained in the Federal Rehabilitation Act of 1973, as amended, which will take effect July 1, 2004 as provided in House Bill 1360 of the 2004 General Assembly session.

Further Considerations: Suppliers should understand that: (i) VITA shall conduct the process for selecting a supplier and negotiating an agreement in such a manner as it, in its sole discretion, shall deem appropriate or desirable (including, for example, negotiating with any prospective supplier and entering into definitive agreements without prior notice to any other suppliers); (ii) any procedures relating to such a transaction may be changed at any time without notice, (iii) VITA shall have the right to reject or accept any proposal or offer, for any reason whatsoever, in its sole discretion; and (iv) suppliers shall not have any claims whatsoever against VITA or any of its respective members, affiliates, agents, or employees arising out of or relating to this request for competitive response or these procedures (other than those arising under a definitive agreement with a supplier in accordance with the terms thereof).

Virginia Partners in Procurement Program
(a.k.a. the Spend Analysis Consulting Services Contract)

James T. Roberts, Director, Department of General Services (DGS), briefed the Committee on the information technology (IT) procurement savings achieved by the Virginia Information Technology Agency's (VITA) participation in the Virginia Partners in Procurement (VaPP) project. The project began after the 2002-2003 economic decline as a way to improve efficiencies for agencies and institutions. Research revealed procurement savings opportunities by consolidating multiple and duplicative contracts, establishing contracts where none existed, better coordinating and leveraging statewide procurement volumes, creating increased competition, and using lower cost substitute items that meet quality and service standards.

The first step in the process was to gather better data on spending. The Commonwealth established eVA, a single point of sale for vendors and state and local government agencies. Sales on eVA have reached between $3 and $3.5 billion on more than 366,000 orders. The next step was to analyze purchasing patterns to effectively leverage the Commonwealth's buying power. For this, the DGS entered into a fixed price contract containing a guaranteed return on investment with Silver Oak Solutions. The project's goals were to create value and savings from spend management and develop collaboration across agencies and institutions, higher education, key municipalities and other public bodies. The project is supported by all levels of government from the Governor and Cabinet Secretaries to key and affected agencies and institutions.

VaPP's three major components consisted of data analysis, contract negotiations and knowledge transfer. Analysis of data revealed key commodities in 17 commodity classes (covering IT and non-IT) accounting for roughly $300 million in annual spending. Then, contract negotiation teams developed specifications for each class, conducted multiple solicitations and requests for proposal (RFPs), met with suppliers, and conducted negotiations to select vendors for each

commodity class. Finally, the vendor transferred the knowledge gained during this project to the agencies as part of an ongoing process of spend management. Ultimately, agency and institution contracting officers are assuming spend management program responsibilities.

The VaPP has resulted in better coordination across government, leveraged statewide purchasing power, a more competitive negotiation processes, increased contract spending with SWAMs, and efficiencies for suppliers. The program continues to emphasize the use and close monitoring of its implementation. The first two waves of the program were run with the vendor. The Commonwealth is now analyzing categories for the third wave, which will be run without consultant assistance. Rebates and surcharges on renegotiated prices are covering the consultant costs and paying the $5 million in contract costs. Despite the surcharges, which will disappear once the contract costs are recovered, agencies still realize substantial cost savings. Participation is increasing as local governments and schools begin to use eVA. Current spending and savings for the last 11 months of fiscal year 2004 were $123.1 million (115 percent of the target) and $15.4 million (127 percent of the target), respectively. Results are expected to increase as purchases through spend management contracts increase. While purchasing through the contracts is strongly encouraged and project leaders were convinced that they had the best price contract, they recognized that there might be a business reason to buy off the contract. They saw stronger use of the contracts even with this built-in flexibility.

Two questions raised by the Committee - the trend of usage for IT through eVA and the percentage or purchases on contract versus off contract – were deferred to another meeting.

Procurement Reform

Mr. Stewart and Susan Woolley, VITA's Director of Supply Chain Management, updated the Committee on IT procurement reform. Chapter 579 of 2002 Acts of Assembly transferred statewide procurement authority for IT and telecommunications goods and services from DGS to the Department of Information Technology. Upon its formation, VITA, one of DIT's predecessor agencies, undertook an IT procurement reform effort to revolutionize the way the Commonwealth purchases IT goods and services.

Mr. Stewart explained that the VITA first had to integrate all IT procurement through eVA to get a handle on IT spending volumes, activity, trends, processes and overall, as well as by agency and by vendor. This information was needed to establish a baseline for spending and to understand the current situation. Comparable size organizations have the information needed to leverage their buying power and the Commonwealth will do the same.

Agencies procure IT in any number of ways. If state contracts were optional, the Commonwealth would not be able to leverage its spending power. Prices would be higher because the Commonwealth could not guarantee any volume to the vendor. To illustrate his point, Mr. Stewart explained that costs for virus software ranged from $9 for a large agency with large volumes to $42 for a small agency with no volume. Therefore, he is proposing mandatory contracts with guaranteed volumes for lower pricing. The process would build in some flexibility with the approval of the CIO if a good business case can be made. VITA will be

developing master contracts for basic hardware and software to achieve quick savings and offset integration costs. The more difficult and complex contracts will come later.

Ms. Woolley explained that the goals of the procurement reform are based on industry best practices. VITA expects to develop an easy to use procurement process with solutions-oriented solicitations, business-driven procurements and performance-based contracts. Prior to the reform, approximately 90 percent of IT procurements were requirements driven and focused only on the best price. The new process will be enterprise-oriented and leverage the Commonwealth's buying power; if the Commonwealth were a corporation, it would rank 50th on the S&P 500. VITA will use the reform to develop partnerships with the vendors that share the risks and benefits, thereby creating opportunities for both.

To meet its goals, VITA reformed the terms and conditions by reducing mandatory terms and conditions to those required by law or by the business owner. All on-line procurements have been consolidated through eVA. VITA also has developed a prequalification process for vendors, mandatory statewide contracts and partnering relationships between itself and its IT suppliers. Among its other achievements this year, VITA executed the first on-line reverse auction for storage media, which yielded substantial cost savings.

The agency also has enabled consistency in ordering IT goods through eVA, which has resulted in better data and more information on the Commonwealth's IT spending. Given the challenge of integrating the IT infrastructure of executive branch agencies, eVA became the common point for all approval requisition processes. The agency will buy what it needs through eVA and the bill will be sent to VITA. This effort requires all agencies to change their existing order and approval processes. DGS is providing the system, training and support to convert the current processes to eVA.

To increase SWAM involvement, VITA is raising awareness among SWAMS by increasing the visibility of opportunities to suppliers and increasing its focus on SWAM objectives. To improve access, the agency is investing in outreach to suppliers and expecting primes to use SWAMs and subcontractors and report on their progress. The new evaluation criteria for contracts considers use and quality of SWAM subcontractors as a factor, though specific targets and goals have yet to be developed. Finally, VITA is tracking the effectiveness of its efforts through communication and feedback. Because SWAMs have indicated that they need more time to respond to solicitations, VITA is giving advanced notice by releasing potential procurement opportunities well before RFPs are issued. VITA has even developed a new website devoted to SWAMs (http://www.vita.virginia.gov/procurement/DoingBusinessW-VITA.cfm).

VITA has developed various procurement processes based on the value (low or high) and need (common or unique). It is currently developing a process to enable agencies to purchase off of the federal GSA schedules, which was authorized during the 2004 General Assembly Session. VITA currently allows use of the GSA schedules in cases of low value and a common need where a direct relationship with the supplier is not needed. While VITA is still gathering all contracts to develop baseline spending and determine volume, preliminary results reveal cost

savings over the next six years of more than $63.4 million that are attributable to the spend management contract and approximately $97.7 million attributable to VITA.

Terms and Conditions of Standardized Contracts

As requested by Delegate Nixon, the Virginia Information Technologies Agency (VITA) provided its standard terms and conditions for information technology procurement contracts. The Committee intends to compare these terms and conditions with the Committee's proposals over the past two years.

Kelley Hellams, Executive Policy Analyst, Supply Chain Management with the Virginia Information Technologies Agency (VITA), briefed the Committee on recent work in standardizing procurement contracts. VITA's new approach to procurement is to memorialize the deal within the contract (i.e. "within the four corners of the document") instead of referencing other documents and provisions, such as the request for proposal (RFP).

Supply Chain Management is in the process of finalizing contract templates for hardware with and without maintenance, service, software licensing, and service level agreements. These new templates move into practice a concept that limits mandatory terms and conditions to those required by the Code of Virginia, and all other terms and conditions will be negotiable. VITA has eliminated as a category "must have" terms and conditions. In addition, the deal, parties and pricing will be readily apparent in the contract, as opposed to being lost within hundreds of pages of supporting documentation.

Ms. Hellams indicated that introducing these contract templates is a significant step towards achieving consistency in contract management. Now, all supply chain management strategic sourcing consultants will have the same starting point regarding contract terms. The contract will no longer be dependent upon the customer or procurement professional. It will be product- and service- driven.

Ms. Hellams provided examples of the new contract terms by setting forth the old and new language regarding warranty services, use of alternative dispute resolution, and confidentiality. These examples demonstrated VITA's attempt to memorialize the deal within the contract to produce more effective contracts. The new contracts focus on using plain and clear language and provide a basis for fact-based negotiation. With the new contracts, one will be able to read the contract and know what is being procured, service level requirements, and the roles and responsibilities of both parties. In addition, the terms are more balanced between the Commonwealth's and supplier's needs. These changes provide the supplier and the Commonwealth with greater predictability by removing the guesswork from contract management and creating more efficient contract administration. The templates incorporate commercially standard contracting language and practices, which is new to state government, but familiar to suppliers.

Introducing the templates is a significant component of moving from traditional procurement to strategic sourcing. The contract is introduced early in the sourcing process and is integral to the

sourcing selection. Procurement professionals will use the contract both in evaluating proposals and in identifying and mitigating risks. They will need fewer resources to reach better decisions in a shorter period of time. Including the contract with the RFPs makes contract negotiation part of the sourcing process, thus promoting effective service level agreements, performance-based contracting, and an expectation that the agreements include ongoing cost reduction and performance improvement.

In addition to VITA contracts, Supply Chain Management is responsible for managing statewide and infrastructure-related information technologies (IT) agreements under VITA's authority through agency transitions. Supply Chain Management asked agencies to submit copies of their IT contract items (i.e., any commitment or ongoing obligation) for analysis. Thus far, it has analyzed over 1,100 contract items. Approximately 400 contract items expired prior to the agencies' transition to VITA and the remaining 700 items have been transitioned. Some of the contract items reflect non-contract purchases, the use of which deprives the Commonwealth of the opportunity to leverage buying power and capture other benefits of consolidation. After the transition of large agencies is complete prior to December 31, 2004, Supply Chain Management will be the central repository for nearly all Commonwealth IT contracts. The contract consolidation process illustrates the need for strategic sourcing.

Ms. Hellams also provided the Committee with an updated copy of its long-term and short-term goals matrix developed and discussed over the previous few years. The Committee identified several goals in procurement that it hoped the newly-formed VITA would address. The updated matrix indicated that the administrative goals within VITA's responsibilities are complete or ongoing, such as establishing a single entity and review process and creating a reasonable limitation of liability clause.

VITA Legislative Proposals

Diane Horvath, Policy and Planning Manager at VITA, presented the Committee with five legislative proposals. She indicated that the agency had not asked the Administration to include these proposals in its package for the 2005 Session. However, it still considered these items ripe for consideration.

The first proposal related to eliminating a preference in the Virginia Public Procurement Act (VPPA) for competitive sealed bidding. Currently to use competitive negotiation, the Code of Virginia (§ 2.2-4303) requires a public body to document, in writing, that competitive sealed bidding is either not practicable or not fiscally advantageous. VITA supports eliminating the written finding and leaving the choice of procurement methodology to the procurement professionals. VITA related that the Department of General Services also supports this change.

The second proposal would amend a public bodies' authorization to purchase IT goods and services through online public auctions or cooperative procurement arrangements. The General Assembly authorized public bodies to procure goods and services from public auctions and cooperative arrangements. VITA's proposal would require a public body to seek approval from the Chief Information Officer (CIO) before pursuing these approaches when procuring IT goods and services. Public bodies already must seek approval from the CIO for procurement of IT

goods and services from other methods, including using the federal General Services Agency's schedules. This proposal would require the approval process for all IT procurements, regardless of the method used.

The third proposal concerned using alternative dispute resolution (ADR). VITA is committed to using ADR as a valid and recognized mechanism to resolve procurement protests, and has successfully used mediation to resolve at least one procurement protest. VITA asked for clear legislative authorization to conduct a three-year pilot project where the agency could promulgate administrative rules requiring vendors to exhaust ADR remedies before filing a protest in court. VITA would collect data about the pilot project to help determine if a more permanent change to the VPPA is warranted. VITA suggests that such a pilot project be authorized for three years.

The fourth proposal addressed a meeting exemption under the Virginia Freedom of Information Act (FOIA). Currently, FOIA provides an exemption for certain proprietary records relating to the Public-Private Education Facilities and Infrastructure Act (PPEA) and the Public-Private Transportation Act (PPTA). It also contains a meetings exemption for discussing the exempt proprietary records that relate to the PPTA. This proposal would amend the meetings exemption to include discussion of the exempt PPEA records, to provide consistency between the existing records and meetings exemptions, as well as between the PPTA and PPEA.

The final proposal requested the codifying, or extending until July 1, 2007, the Act of Assembly implementing electronic meetings. Currently, the Information Technology Investment Board, the Virginia Geographic Information Network Advisory Board and the Wireless E-911 Services Board use these provisions. The Committee already began examining this issue.

The Committee did not endorse any of the proposals, but instead recommended them for further review by JCOTS. Regarding the ADR pilot project, Delegate Nixon cautioned that any legislation should include a provision that would allow a protestor to proceed directly to court if pursuing ADR would cause an undue burden, such as financial hardship.

Public Safety Interoperability Coordination

Chris Essid, Commonwealth Interoperability Coordinator for the Office of the Secretary of Public Safety, explained the development of the Commonwealth's Strategic Plan for Communications Interoperability. While Mr. Essid's office is located within the Office of the Secretary of Public Safety, he works across the Secretariats to address interoperability issues throughout government. Being the first state in the nation to create a governance structure for interoperable communications, the Commonwealth serves as a model for the nation.

Mr. Essid began by providing background on the issue and the SAFECOM program. Inadequate and unreliable wireless communications have been issues plaguing public safety organizations for decades. In many cases, agencies cannot perform their mission critical duties. These agencies are unable to share vital voice or data information via radio with other jurisdictions in day-to-day operations and in emergency response to incidents including acts of terrorism and natural disasters.

According to a report done by the National Task Force on Interoperability (February 2003), the public safety community identified several key issues that hamper public safety wireless communications today - incompatible and aging communications equipment; limited and fragmented budget cycles and funding; limited and fragmented planning and coordination; limited and fragmented radio spectrum; and limited equipment standards. In short, the nation is heavily invested in an existing infrastructure that is largely incompatible. The federal Office of Management & Budget established the SAFECOM Program and the President's Management Council approved it to address these public safety communications issues.

SAFECOM's mission is to serve as the umbrella program within the federal government to help local, tribal, state, and federal public safety agencies improve public safety response through more effective and efficient interoperable wireless communications. Communications interoperability is the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, when authorized.

As a public safety practitioner driven program, SAFECOM is working with existing federal communications initiatives and key public safety stakeholders to address the need to develop better technologies and processes for the cross-jurisdictional and cross-disciplinary coordination of existing systems and future networks. SAFECOM harnesses diverse federal resources in service of the public safety community. SAFECOM makes it possible for the public safety community to leverage resources by promoting coordination and cooperation across all levels of government. The program has developed standardized grant guidance for public safety interoperability equipment grants and is working for standardized grant guidance for all interoperability grants, assisted the Commonwealth with the development of the Statewide Interoperable Communications Strategic Plan and governance model, and developed best practices to assist other states in developing interoperability plans.

In developing a strategic plan, Mr. Essid's office held focus group sessions in rural and urban areas around the Commonwealth. The focus groups afforded the Commonwealth the ability to capture the perspective of the local responders on interoperable communications, share education and awareness with all stakeholders, and learn the commonalities and differences among the regions. Feedback from these focus groups established an understanding of the current state of interoperability and the barriers standing in the way of future goals to make a case for change. The goals of these sessions were to establish communications interoperability as a high priority in the Commonwealth, establish the statewide use of a common language and coordinated protocols for emergency response, maximize interoperability capabilities using existing systems and equipment and planning for future technology purchases, and enhance knowledge and use of existing and future systems and equipment. At a strategic planning session, stakeholders reviewed the information from the focus groups and used that information to develop the core components of the strategic plan.

The barriers that emerged involved a lack of priority, lack of coordination, lack of lifecycle planning, technical barriers, inadequate training and numerous statewide mutual aid channels. Inconsistent funding streams and insufficient personnel resources allocated to drive collaboration demonstrates a lack of priority for interoperability. The use of different codes and terms and

inadequate coordination of standard operating procedures evidences a lack of coordination. Current barriers to lifecycle planning include artificial lifecycles established by vendors and built-in incompatibility between versions of systems. Many grants do not pay for training creating a problem when implementing new systems. Finally, with various systems in place statewide and a lack of funding to replace all of them, the Commonwealth needs a "system of systems." Mr. Essid highlighted that the true problem with coordination is only 10 percent technology and 90 percent people.

The goal is to establish interoperability as a high priority in the Commonwealth with common standards, a common approach to lifecycle planning and extensive training and information sharing. To further this goal, Governor Warner established the Commonwealth Interoperability Coordinators Office (CICO). CICO will coordinate projects and efforts across the Commonwealth, act as a liaison with the Commonwealth Preparedness Working Group, act as a conduit between Initiative Action Teams and others and monitor their progress, and request resources, as required. CICO will receive advice and recommendations from the First Responder Interoperability Executive Committee. Ten representatives of state and local government and the public safety community comprise the Executive Committee and will receive support from a larger Advisory Committee.

Mr. Essid reported that the Governor approved the strategic plan, which he will introduce at the Statewide Interoperability Communications Conference in Richmond on October 19-20. The Conference is an opportunity for public safety responders to get together to discuss interoperable communications. Work will continue to secure funding to implement the initiatives, and the CICO will solicit applications to award $2.4 million for local interoperability grants.

Electronics Recycling

Daniel G. “Bud” Oakey, CEO of Advantus Strategies and member of the Committee, discussed asset recovery (i.e., electronics recycling). According to Dell Corporation’s research, 95 percent of all new personal computers (PC) replace existing systems, and 88 percent of customers have excess computer equipment. With all of these systems to dispose, 68 percent of customers are unaware of how to do it and 52 percent do not know how to address environmental liabilities. Storing these systems can be costly not only because of the wasted space, but also because the average cost of storing a PC for one year is $450 with a six percent per month depreciation rate.

Any type of electronics can be recycled and numerous companies have programs. According to the Aberdeen Group, three reasons outline the need to recycle electronics: cost/value, data security and environmental concerns. If stored IT equipment has any value, rapid depreciation dissipates it; if it has no value, it constitutes a pure storage cost. Either way, the sooner the equipment is disposed of, the greater the gain. The equipment may contain sensitive or legally protected information raising the risk of liability or business harm. Effective sanitation of drives, while labor intensive, must be done to reduce this foreseeable business risk. Finally, obsolete electronic devices contain hazardous materials that are not wanted or allowed in dumpsters and landfills. The ability to track and comply with the ever-changing regulations governing this material is crucial.

Mr. Oakey cautioned that existing procurements consider only acquisition issues and not disposition. However, public policy should consider the entire lifecycle cost from acquisition to disposition. As part of this consideration, he recommended that procurement contracts be modified to include disposition. Mr. Oakey noted that all of the companies from which the Commonwealth currently procures offer asset recovery services and would be more than happy to pick up competitors' equipment to replace with their own, which is also covered by their programs.

Among the programs discussed or presented were those operate by Dell, Nextel, IBM, and Gateway. In 2003, Dell hosted recycling events in 17 U.S. markets and collected nearly two million pounds of electronic waste. Dell is also working to minimize and eliminate use of materials that are environmentally sensitive, to reduce the impact that its facilities have on the environment and to reach out to customers and provide them with needed information. Dell developed the Sustainable Business function in 2003 to ensure the integration of social and environmental concerns into its business operations and interactions with stakeholders while ensuring that its economic goals are met.

With an estimated 60 million handsets sitting idle, Nextel has developed a Refurbishing and Recycling Program ($NexR^2$) that encompasses all aspects of used equipment handling, including collecting, refurbishing and recycling cell phones. Customers who participate can receive account credit or a tax deduction by donating their phones to the Red Cross. To make participation convenient, Nextel offers customers the ability to print out prepaid FedEx labels through the company's website or to return phones to retail stores, service centers or even NASCAR events. Once received, the company separates phones from the usable, which will be refurbished, to the waster, which will be disposed of or reused for other uses. The company also uses phones to support internal programs and marketing. Like Dell, Nextel is looking for new ways to reuse, repurpose, refurbish and recycle phones.

IBM, Gateway, and many more companies offer similar services to recycle or dispose of unwanted information technology assets. Benefits to using these programs include door to door shipping services, credits for assets that still have value, and assurances that data will be completely cleaned from devices. Widespread use of these programs requires a change in mindset and procurement practice in the Commonwealth.

Certified E-Mail

Fred Norman, Principal of Commonwealth of Virginia Consulting and a member of the Committee, apprised the Committee of a relatively new service called certified electronic mail (e-mail). South Carolina provided in its recently adopted Uniform Electronic Transactions Act (UETA) that e-mail using the United States Postal Service (USPS) electronic postmark (EPM) service is a legal alternative to certified or registered U.S. mail for certain types of electronic communications, and carries the same force of law and legal effect as those physical mail services. UETA provides a legal framework for electronic transactions, and gives electronic signatures and records the same validity and enforceability as manual signatures and paper-based transactions. Specifically, the legislation states that the "United States Postal Service electronic postmark means an electronic service provided by the United States Postal Service that provides

evidentiary proof that an electronic document existed in a certain form at a certain time and the electronic document was opened or the contents of the electronic document were displayed at a time and date documented by the United States Post Office."

Mr. Norman explained that the USPS EPM protects the integrity of electronic data through the use of auditable time stamps, digital signatures and hash codes and enables any third-party to verify the authenticity of electronic content. He indicated that with VITA as the agency of centralized ownership of a digital authentication program and the USPS EPM system, the Commonwealth has the ability to implement an enterprise solution for itself and its citizens to further conduct electronic transactions in a secure and trusted environment.

Uniform Electronic Transactions Act (UETA)

Committee members unfamiliar with UETA received a brief summary of the Act. The National Conference of Commissioners on Uniform State Laws proposed UETA to enable electronic commerce by providing that electronic contracts, records and signatures could not be denied legal effect or enforceability solely because they were in electronic form. At least 42 states plus the District of Columbia have adopted UETA in one form or another.

Outsourcing & Offshoring

Staff provided the Committee with a briefing on outsourcing, in general, and, more specifically, offshoring by government entities. State and national governments, including the Commonwealth, have focused on the issue and its impact on the domestic economy, especially on jobs.

Generally, outsourcing involves a company turning over responsibility, in whole or in part, for an internal business function to an outside service provider. Government can outsource by hiring a vendor through the procurement process to perform a task or service that it traditionally has performed. While outsourcing is nothing new, the model for outsourcing has become increasingly global. This leads to a discussion of offshoring, where labor is performed in another country, and the business process is moved to a lower-cost location, usually overseas. In large part, improvements in technology such as fiber optic cables and the Internet have lowered communication costs and made offshoring economically feasible. While all sectors now face offshoring of jobs and functions, the most common types of jobs include customer service, call service operations and data entry. The key policy questions that emerge for government involved with or considering involvement with companies that offshore are (i) the acceptability of spending tax dollars overseas if it saves money and (ii) whether the state has an obligation to ensure that tax money stays in the domestic economy.

Offshoring is increasingly controversial, and arguments abound both in favor of and in opposition to the practice. Proponents of offshoring argue that it increases the number of American goods in foreign markets, encourages free trade, increases competition, and creates a new demand for goods often purchased in the United States, such as computers. Proponents also suggest that the increased earnings of a domestic company offshore will be repatriated and

returned to the United States through taxes. In the public sector, the lower cost of offshoring promotes more efficient spending and effective utilization of tax dollars. They argue that most often, lower-level jobs are offshored, opening the door for the development of more advanced, higher-paying jobs domestically. Finally, they suggest that implementing prohibitions against offshoring might lead to economic retaliation by other countries and could hamper the general administration of public sector outsourcing.

Opponents of offshoring counter that losing jobs overseas is generally bad for the economy. More specifically, they argue that while offshoring appears to save money, there are often hidden costs such as higher general operations costs, the costs associated with shutting down domestic facilities, and social services costs to the state through unemployment and job retraining. Additionally, they argue that cultural differences, language barriers, and potential political instability in foreign countries may create business problems. Opponents suggest that although typically lower-level jobs are lost to offshoring, technology makes it possible for "white collar" jobs to be offshored as well, and there is no guarantee that increased profits or savings will be used to support the growth and development of new domestic jobs. Finally, opponents raise questions about data security. While a company subject to U.S. jurisdiction must comply with state and federal laws (e.g., intellectual property laws, employment protections, consumer protection laws, telemarketing restrictions, the Fair Credit Reporting Act, and privacy laws like the Gramm-Leach-Bliley Financial Modernization Act (GLB), the Health Insurance Portability and Accountability Act (HIPAA)), concerns emerge surrounding the process and security of moving and rerouting data outside of the United States. Companies also may lose their protections under the safe harbor exemptions to European privacy laws, hindering their ability to process data on Europeans. The Federal Trade Commission has argued that U.S. companies deciding to conduct activities offshore and their third-party providers still are subject to U.S. privacy and consumer protection laws.

In response to these concerns, more than 35 states and the federal government have proposed several pieces of legislation. Approaches include giving preferences to domestic vendors in the procurement process, prohibiting work with companies that offshore, placing restrictions on offshore call centers, limiting the processing of certain data abroad, or providing tax benefits to companies that keep jobs in the United States. Tennessee became the first state to pass such legislation. That law is specifically targeted towards data entry and call centers. Other states have issued executive orders or resolutions "encouraging" companies to keep employment in the United States or in a particular state.

The Virginia General Assembly introduced four bills during the 2004 General Session that addressed outsourcing and offshoring. Committees continued all of these bills to the 2005 General Session. House Bill 243 (Patron - Nutter) and Senate Bill 151 (Patron - Deeds) would create a preference in the procurement process for goods produced in the United States or services provided by U.S.-based companies, so long as the bid price was not more than 20 percent greater than the lowest responsive bid. House Bill 315 (Patron - Cosgrove) would give a three percent preference to goods manufactured, developed or produced in Virginia for contracts in excess of $500,000. House Bill 1010 (Patron - Rust) would prohibit a public body from entering into a contract for professional services unless the contract provides that only United

States citizens, legal resident aliens, and individuals with valid visas will perform the services under the contract or any subcontract.

Electronic Communication Meetings

Staff briefed the Committee on provisions relating to electronic communication meetings in Virginia. Section 2.2-3708 of the Virginia Freedom of Information Act (FOIA) enables any state public body to hold a meeting via audio or audio/visual means, so long as it follows certain provisions. The provisions include such requirements as 30 days notice for a meeting held via electronic communication means, and that a quorum of the membership must be physically assembled in one location before other members can meet from remote sites. Those remote sights must be located in Virginia and be open to the public. In addition, the provisions limit a public body to holding no more than 25 percent of its meetings annually via electronic communication means. The legislature enacted these provisions in 1989, and they basically remain unchanged.

In 1999, however, the General Assembly enacted Chapter 704 of the Acts of Assembly of 1999, which contains alternative provisions with lessened requirements (known as "the Pilot Project"). The Pilot Project applies only to certain state public bodies holding audio/visual meetings. Its provisions require only seven days notice of such meetings, and only three members of a public body (or a quorum if less than three) must be at sites that are both in Virginia and open to the public, although these three members do not necessarily need to be at the same physical location. Once the presence of three members, or the quorum, is established, other members may meet from locations not in Virginia or not open to the public. Because the General Assembly intended the Pilot Project to be a temporary project to gather data on how the lessened requirements affected public access to meetings, it also contains heightened reporting requirements concerning the meetings. The Pilot Project will expire July 1, 2005 absent legislative action by the 2005 General Assembly.

Susan Hayden, Director of Public Affairs for the Virginia Community College System (VCCS), provided her agency's experience with electronic communications meetings to the Committee. Ms. Hayden indicated that the VCCS Board frequently uses the Pilot Project provisions when nominating candidates for president of one of the community colleges. She noted that this process usually occurs outside of the timeframe of regularly scheduled Board meetings. The Board's members are located around the Commonwealth, and these meetings only last about 15 minutes. Because the Pilot Project uses a "dispersed quorum" requirement, where the members may participate remotely from sites around the Commonwealth, as opposed to being physically assembled in one location, VCCS saves money and time. Additionally, Ms. Hayden reported that VCCS experiences increased public participation from the media and citizens during electronic communications meetings than during regularly scheduled Board meetings where the members physically assembly at the meeting location. Because of VCCS's positive experience, Ms. Hayden indicated that it would support a measure to adopt the "dispersed quorum" requirement, or, at least, to extend the sunset provision on the Pilot Project.

Staff recommended that the Act establishing the Pilot Project be allowed to expire, and that Committee consider amending FOIA to create one set of requirements incorporating provisions

from the Pilot Project. Practical experience indicates that many public bodies do not take advantage of the FOIA provisions because some of its requirements are stringent; however, because the Pilot Project does not apply to all state agencies and enables only audio/visual conferencing, many state agencies do not take full advantage of it, either. Furthermore, because the Pilot Project only appears in the Acts of Assembly and the annotations to the Code of Virginia (annotations are not available online), many public bodies do not realize that it exists. Creating one standard for electronic communication meetings that addresses some existing logistical concerns will provide for more use of such meetings and may increase public participation in these meetings. The Committee voted to adopt these recommendations. However, it also voted to remove the requirement that electronic communications meetings be recorded.

The final proposal would amend § 2.2-3708 to (i) reduce the notice requirement from 30 days to seven working days; (ii) count toward a quorum of the public body those members present at locations in Virginia and open to the public; once a quorum is established, other members may meet from remote locations outside of Virginia or not open to the public; (iii) require that reports be filed annually with JCOTS and the FOIA Council identifying experience and issues with the meeting; (iv) eliminate the recording requirement; (v) allow closed meetings to be held via electronic communications; and (vi) eliminate the limit on the number of meetings that can use electronic communications.

Staff of JCOTS also met with a subcommittee of the Freedom of Information Advisory Council that was also considering legislation relating to electronic meetings. JCOTS staff shared the Committee's initial proposal with the FOIA subcommittee to discuss their positions on the issues.

The FOIA Subcommittee's proposal contained some provisions identical to the JCOTS Advisory Committee proposal, such as shortening the notice required for electronic meetings to seven working days and eliminating the provisions allowing a public body to hold only 25 percent of its meetings annually using electronic communications. The FOIA proposal also included provisions requiring posting the notice on the Internet, including a contact phone number in case of technical difficulties, and requiring the public bodies to hold at least one physical meeting a year (in lieu of the 25 percent limitation). The FOIA Subcommittee agreed to recommend most of JCOTS' proposals to the FOIA Council. However, the proposals differed in two provisions - (i) whether to require that a quorum be assembled in one physical location or allowing it to be dispersed across locations in Virginia that are open to the public, and (ii) whether all remote sites must be open to the public. The FOIA draft required a physically assembled quorum with all remote sites open to the public; the JCOTS draft allowed a disperse quorum and did not require that all remote sites be open.

The Committee incorporated all of the FOIA Council's proposals that did not conflict with its initial draft into its recommendations to JCOTS. However, it retained the disputed provisions, and suggested that JCOTS continue discussing them. (See Appendix 5.)

C. NANOTECHNOLOGY

- **Delegate Purkey, Senator Wampler, and Delegate Cosgrove, co-chairs**

HJ 120, adopted by the 2004 General Assembly, directs JCOTS to identify nanotechnology research and economic development opportunities for the Commonwealth and consider the efficacy of creating a statewide, comprehensive and coordinated strategy to secure additional federal research and development funds and to boost commercial activity in this fast-emerging sector. JCOTS created the Nanotechnology Advisory Committee to conduct this study.

The committee met three times during the 2004 interim, on August 4, September 22 and October 20. During its meetings, the Committee received briefings on nanotechnology issues, state and federal nanotechnology initiatives and the competitive landscape, and a proposed Nanotechnology Accelerated Development Center. Committee members also had the opportunity to share their individual backgrounds and views of nanotechnology.

"Five Good Minutes": Member Introduction

Because of the diverse backgrounds and expertise represented on the Advisory Committee, each member introduced themselves, talking about their backgrounds, their employers, nanotechnology affiliations, and goals for nanotechnology in the Commonwealth.

• Dr. Richard Claus is Director of the Fiber and Electro-Optics Research Center at Virginia Tech. He focuses on making nanomaterials on a macro level. He suggests focusing on the key areas of teaching and education, research (including graduate research) to generate intellectual property, and outreach involving spinning off intellectual property and creating small companies.

• Steve Danziger is a Program Manager at BAE Systems and a member of the Northern Virginia Technology Counsel's Nanotechnology Committee. Having been involved for more than 20 years in many aspects of state-of-the-art semiconductor technology from engineering to executive management, he is currently integrating carbon nanotube technology to create an improved semiconductor memory device. His goal is to see increased involvement and investment in nanotechnology by established Virginia companies and further collaboration among government, academia, and private organizations to facilitate the commercialization of nanotechnology in Virginia. In addition, he would like to see a Virginia nanotechnology center of excellence established, involving several organizations.

• Dr. Frederick Dylla is the Chief Technology Officer and Program Manager of the Free-Electron Laser (FEL) project for the Thomas Jefferson National Accelerator Facility. He ensures awareness of new and developing technologies that could be used to enhance or improve Jefferson Lab's (JLab) scientific program; and he leads JLab's Technology Transfer team to identify commercialization opportunities for Lab-developed technologies. As the FEL program manager, he is responsible for Jefferson Lab's Free-Electron Laser, a major initiative funded

through the Office of Naval Research that uses Jefferson Lab's key technology (superconducting radiofrequency cavities) to produce high average power, coherent light. The lab recently undertook an $80 million project to build the world's most tunable laser. He noted that the Lab frequently interacts with Virginia universities and companies, an essential element of continued nanotechnology development.

• Charles Gause is the Vice President of Luna Innovations Inc.'s Danville Division, a company that specializes in commercializing research from the laboratory. Luna Innovations recently renovated an 1870s tobacco warehouse to create a state-of-the-art nanomanufacturing facility. He acknowledges Virginia's tradition of academic and industrial excellence as a means to aid in nanotechnology development efforts for current and emerging industries. He believes that issues critical to the growth of nanotechnology in Virginia include cost effective manufacturing of nanomaterials as an economic growth opportunity, development of a nanomanufacturing workforce, and a unified Virginia information exchange network for nanotechnology business development.

• Daniel Gonzalez is Executive Vice President and Managing Principal of Scheer Partners, Inc., a regional commercial real estate consulting firm that specializes in advising biotechnology, technology and microelectronics firms. He is also a member of the Northern Virginia Technology Council and Governor Warner's Biotechnology Advisory Board. He is interested in creating a sound strategy to capitalize on the convergence of technologies to benefit the overall economic development of the Commonwealth.

• Dr. Richard Gregory is Professor and Dean for the College of Sciences at Old Dominion University. He has a background in organic electronics and material sciences. He sees a need for a focus in Virginia to allocate resources and provide funding to build areas in which the Commonwealth can succeed. One of the goals of a nanotechnology program should be to keep graduates from Virginia schools in the Commonwealth.

• Dr. Frank Gupton is an organic chemist and is the Technical Director in pharmaceuticals at B.I. Chemicals. He noted that there is a trend in the chemical and pharmaceutical industries of increasing levels of molecular complexity in new drugs, and nanotechnology can help to develop new catalysts in the future. Drug delivery systems are being developed to help better supply the active ingredients and a better understanding of the molecular level of the ingredients will help in the development. He sees nanotechnology as an enabling technology that applies to other systems to aid in better understanding.

• Dr. Robert Hull is the Charles Henderson Professor at the University of Virginia, Director of a program on "Nanoscopic Materials Design" that is funded by the National Science Foundation as part of its Materials Research Science and Engineering Center (MRSEC), and Director of the University of Virginia Institute for Nanoscale and Quantum Engineering, Science and Technology. He believes that a key focus should be winning nationally competitive Center awards within state universities. These programs demonstrate excellence, generate substantial follow-on funding, help build infrastructure, will help build a nano-economy in Virginia and will greatly enhance external perceptions. A key strategy is developing partnerships across institutions, thus enhancing the pool of talent and facilities. State funding can help greatly in

building the infrastructure to enable us to compete against the nation's leading institutions on a level playing field.

• Dr. Dimitris Ioannou is a professor in the Electrical and Computer Engineering Department at George Mason University. He has a strong physics background, and works closely with the graduate and undergraduate programs. He has been trying to tailor a curriculum to develop a graduate certificate program in nanotechnology, and has begun to offer a few classes this semester.

• Dr. Philip Lane practices Intellectual Property law with McGuireWoods and has a Ph.D. in Chemistry. A key question for him is whether the Commonwealth is protecting what it is developing. For developments in nanotechnology to attract business to the Commonwealth, the intellectual property resulting from it must be protected.

• Dr. Dennis Manos is the CSX Professor of Physics and Applied Science at the College of William & Mary. He serves as the Vice-Provost for the College, with primary responsibility for research, graduate, and professional study. His interest in nanotechnology began with work on soot formation in the late 1970s, and his current research includes plasma processing techniques, production of field emission devices from patterned carbon nano-structures, development of clinical diagnostic methods for identification of diseases by analysis of serum and tissue protein and peptide markers, and computational methods for enhancing very large data streams. The College is part of the part of the consortium that operates the Applied Research Center in Newport News, which has been in full operation since 1998 and has aggregated university resources to initiate collaborative research. He reiterated William & Mary's firm commitment to continued work in this important area and its willingness to invest in developing shared infrastructure to bring this promise to reality.

• Dr. Robert Mattauch is Dean of the School of Engineering at Virginia Commonwealth University. He initiated semiconductor device work at the University of Virginia in 1966, and by the time he left the program boasted 11 Ph.Ds. and 47 graduate students. He explained that the development of inorganic crystalline semiconductor materials reduced the size of satellite dishes from 14 feet to 14 inches, while transforming them from analog receptors to digital and led to the development of collision avoidance radar. Advances have reduced the energy required for magnetic storage by a factor of ten million (10^7), and led to the development of polymeric surfaces that can detect toxins and the growth of veins and tissues that are 100th the width of a human hair using bioscaffolding. He emphasized that the Committee must focus on stimulating and growing nanotechnology manufacturing. This focus requires a careful balance of university research and industrial input and support. He warned that the Commonwealth must be wary of research "chameleons" who rename their work to correspond with the latest highly funded area of research. True nanotechnology involves research at such a micro level that the properties of the material change and not merely macro research on the micro level.

• Scott McNeil is a scientist at Science Applications International Corporations (SAIC)'s Systems Integration Department. Through his association with SAIC, he has worked with the Nanotechnology Cancer Lab and the National Cancer Institute. He believes that it is critical for the Committee to address and define what it wants to accomplish with nanotechnology.

• Dr. John Noftsinger is the Associate Vice President of Academic Affairs for Research and Public Service and Executive Director of the Institute for Infrastructure and Information Assurance at James Madison University (JMU). He has a background in policy and experience in working collaboratively with other universities. JMU currently has several ongoing activities around campus that have caught the eye of industries. He suggested creating a Nanotechnology Commission much like the Governor's Biotechnology Advisory Board. He also suggested funding the Commonwealth Technology Research Fund, which has been instrumental in encouraging university collaboration. If funded, it could provide a vehicle for future collaborations. Dr. Noftsinger noted that JMU used the grant to work with George Mason University and obtain federal funding for the Critical Infrastructure Protection Project.

• Victor Peña is co-Founder and CEO of nanoTITAN, Inc., company that develops software for nanotechnology companies. He is a member of the President's Council of Advisers on Science and Technology and its Nanotechnology Technical Advisory Committee, co-Founder and Steering Group Member of InanoVA (VNI), and co-Chair and co-Founder of the Northern Virginia Technology Council's Nanotechnology Committee. His goal is for the Committee to produce a business plan of policy and legislative actions for the Governor and legislators that identifies actions and resources in the Commonwealth that are necessary to build a nanotechnology economy. This plan should include a SWOT analysis (a SWOT analysis involves a scan of the internal and external environment assessing strengths, weaknesses, opportunities and threats), funding requirements and sources, academia, K-12 education, federal and state resources, tax incentives, technology transfer streamlining, attracting nanotechnology businesses to the Commonwealth, public relations, and promotional conferences. He suggests that the Committee should exercise systems engineering and life cycle principles in this endeavor.

• Dr. Mark Shuart has worked for the NASA Langley Research Center since June 1977, and currently is the Director of Structures and Materials. The Langley Research Center is widely recognized for its technical expertise in aerospace. As part of that capability, the NASA Langley's structures and materials organization has been identified as the Agency's Center of Excellence in that discipline. The structures and materials organization participated in orbiter tile research in the early 1980's, helped analyze the Challenger accident and return the Shuttle to flight and assisted the National Transportation Safety Boarding in the accident investigation for American Airlines 587. The Structure and Materials organization includes more than 250 researchers working in facilities valued in excess of $400 million, and the products of their research have found numerous aerospace and non-aerospace applications.

• Robert Smartschan is a partner with the law firm of Kaufman & Canoles. As the founder of the firm's Technology Ventures Group, he helps clients protect business assets under intellectual property laws and concentrates on technology licensing and transfer, and similar matters. He is a member of the Board of Directors for the Hampton Roads Technology Council, and serves as General Counsel to the Hampton Roads Technology Incubator, a facility whose mission is to nurture early stage high-tech companies into profitable industry leaders. Mr. Smartschan is interested in the developing nanotechnology as a viable contributor to Virginia's economic expansion, especially in the Hampton Roads region.

• Richard Smith is the President of Nanotechnology Network, co-founder of the Nanotechnology Policy Foundation, and Principal in Nanoverse, LLC, a nanotechnology commercialization firm. The Nanotechnology Network was created to foster collaboration among Maryland, the District of Columbia, and Virginia and develop a regional nanotechnology initiative. The Nanotechnology Policy Foundation fosters public dialog about the societal implications of nanotechnology and hopes to become an "honest broker" for the public, policymakers, and the press. Nanoverse focuses on commercializing intellectual property developed by universities, though currently none in Virginia, in the fields of health and medicine, energy, and homeland security.

• Dr. Sharon Smith is the Director of Advanced Technology for Lockheed Martin Corporation, a member of the Northern Virginia Technology Council, and a member of the Board of the NanoBusiness Alliance. At Lockheed Martin, a developer and integrator of technology, she focuses on applications for homeland security and defense. For the growth of nanotechnology in Virginia, she considers facilitating the interactions between local government, academia, large corporations and small businesses to be most important. The Commonwealth must address educating the current and future workforce and establishing financial incentives for nanotechnology start-up companies.

• Bruce Swenson is Founder and co-Chair of the Northern Virginia Technology Council's Nanotechnology Committee and a systems engineer at the Science Applications International Corporation (SAIC). He emphasized the cross-disciplinary nature of nanotechnology and the need for cross-regional cooperation. The Commonwealth must acknowledge that nanotechnology is capital intensive and requires multi-disciplinary collaboration as well as shared equipment and expertise, and its strategy should include facilitating collaboration on the state, federal, and international levels. Virginia should focus on developing the entire spectrum of nanotechnology, from research to prototyping to manufacturing. The Commonwealth's strategic position (proximity to a large government customer base) can encourage companies to establish a presence here.

• Dr. Usha Varshney is Acting Director of the National Science Foundation's (NSF) Electrical and Communications Systems Division. NSF is an independent federal agency that helps set and advance the national agenda for research and education in science, mathematics, engineering and technology. The agency supports basic research and education through the grant mechanism based on peer review. For FY 2004, the Foundation funded research and education in nanoscience, nanoengineering and nanotechnology with $253 million; the President authorized $385 million for FY 2005.

• Charles Wieland is a co-founder of the Atlantic Nano Forum, an organization created to facilitate the training of patent examiners in nanotechnology. He is also a partner at the intellectual property firm of Burns, Doane, Swecker & Mathis, LLP in Alexandria. Mr. Wieland would like to find more ways to encourage universities and federal labs to spin-off nanotechnology based companies in Virginia.

Introduction to Nanotechnology

Dr. Robert Hull, Director of the NanoQuest Institute and Professor of Engineering, University of Virginia, presented an overview of nanotechnology. Nanotechnology involves the ability to engineer systems with components on length scales of one to 100 nanometers (a nanometer is a billionth of a meter). To put the size into perspective, a two-meter tall human is two billion nanometers tall and a pinhead is a million nanometers in diameter. Biological cells, like red blood cells, have diameters in the range of thousands of nanometers. Ten shoulder-to-shoulder hydrogen atoms span one nanometer, while DNA molecules are approximately two and a half nanometers wide. Individual atoms are up to a few angstroms, or up a few tenths of a nanometer in diameter. Properties and structures at these reduced scales often are different and better. The ability to make things smaller means that they are cheaper, lighter, and use less power to operate.

Nanotechnology has reached major importance today because scientists have developed the capabilities, such as computational, fabrication and measurement methods, to exploit materials, as well as an improved understanding of nanoscale biological processes. Through new techniques, they have been able to develop new materials and phenomena. Finally, they have been able to prove the impact of these new techniques on industries with tens of billions of dollars in annual sales, a major impact on the economy.

Money helps. In December of 2003, the federal government enacted the 21st Century Nanotechnology Research and Development Act (S.189) authorizing almost $3.7 billion in government funding for nanotechnology research and development (R&D). The legislation emphasizes the establishment of R&D Centers in academia and government. There are now over 50 institutes and centers dedicated to nanotechnology research. For example, the National Science Foundation has established the National Nanotechnology Infrastructure Network - comprised of 13 university sites that will form an integrated, nationwide system of user facilities to support research and education in nanoscale science, engineering and technology. Similarly, there are currently 15 government agencies with R&D budgets dedicated to nanotechnology. Opportunities exist for numerous industries such as electronics and optics, healthcare, the environment, energy, microspace, bio-threat detection, transportation, and national security.

These new abilities already have enabled the creation of smaller devices, a greater capacity for data storage, the creation of new catalyst materials and increased capacity on semiconductor wafers. Other existing applications include high performance sports equipment, specialized auto and aero components, polishing powders and slurries, stain-free fabrics, sun tan lotion and cosmetics, selective optical coatings (e.g., photographic film), telecommunications components, machine tools and corrosion and scratch resistant paints and coatings. To illustrate nanotechnology's potential impact on the world, if the aircraft industry had evolved at the same rate as the microelectronics industry in the last 25 years, a Boeing 777 today would cost $500, and circle the globe in twenty minutes on five gallons of fuel.

Major new opportunities exist for the Commonwealth in nanotechnology, such as the development of new methods for self-assembly of materials, based upon both biological and non-biological methods and the creation of new materials, methods, and instruments for harnessing sub-atomic properties. Opportunities also exist for the development of improved

instruments and techniques for structuring and patterning materials at ever-increasing levels of precision and the ability to measure the three-dimensional structure, properties, and chemistry of materials down to the atomic scale, a sort of a "nano-GPS." Researchers also will be able to take advantage of the interface between nanomaterials and biological systems, enabling widespread improvements in human health.

Other major future impacts exist in the fields of electronics and computation; communications; data storage; energy storage, transmission and generation; health care; transportation; civil infrastructure; military applications and national security; and the environment. Emerging and future applications for the automotive and aeronautic industries include nanoparticle-reinforced materials for lighter, stronger bodies, nanoparticle-reinforced tires, self-cleaning and –repairing materials, electronics, and collision avoidance. In electronics and communications, applications include an extension of Moore's law to thousands of times higher density, speed, lower power consumption and cost and the development of magnetic nanoparticle media. For chemical materials, they include improved catalysts, smart magnetic fluids for vacuum seals and lubricants, self-cleaning and –repairing surfaces, and adaptive surfaces. In health care, they include nanostructured drugs, gene and drug delivery systems targeted to specific sites in the body, biocompatible replacements, self-diagnostics, bone and tissue regeneration, and wound repair. Impacts on energy technologies include higher power density batteries, fuel cells, artificial photosynthesis, improved solar cells, improved fuel economy form lighter materials, and improved electronics. In manufacturing, they include super-hard and –tough cutting tools, ultra-precision engineering based on nanoscale microscopies, atomic-scale manufacturing tools and processes, nanopowders, internal sensors for fault detection and repair, and self-assembling materials. In space exploration, opportunities include lighter vehicles, improved energy generation, ultra-small robotic systems, in-flight sensing and repair capacity. For the environment, possibilities include reduced pollution through catalysis, nanostructured traps for pollutant removal, improved recycling, selective membranes for water filtering, and cleaner manufacturing processes. National security opportunities include detectors and detoxifiers of biological and chemical agents, improved electronic and optical systems, radiation-protected systems, harder coatings and bodies, camouflage materials, improved textiles, self-repairing materials, and in-battle medical care.

Economists estimate that the world market for nanotechnology will equal $1 trillion by 2015 and create 800,000 to 900,000 jobs. In Virginia, opportunities exist for partnerships in research, manufacturing, and education. Dr. Hull suggested that the Commonwealth can capitalize on existing research facilities and their expertise, lead educational programs, and grow its nanomanufacturing base. To capitalize on the possibilities, he stressed four issues that the Commonwealth must evaluate: (i) how these advances affect education at all levels (K-12, undergraduate, graduate, and beyond); (ii) how the Commonwealth can use nanoscience to educate and inspire society to be technologically literate; (iii)how it can encourage educational institutions to value and reward interdisciplinary programs; (iv) and how it can perform high-risk, high-cost research that will also benefit societies, or portions of societies, that cannot afford it. Finally, a real-life argument for focusing on nanotechnology is the sustainability of expected population growth over the coming decades.

Nanotechnology: Achieving Leadership in Virginia

Dr. Lisa Friedersdorf, Director of the Virginia Nanotechnology Initiative, and Ms. Nancy Vorona, Vice-President of Research Investment at the Center for Innovative Technology (CIT), briefed the Committee on achieving nanotechnology leadership in Virginia. Their presentation focused on key questions that the Commonwealth must answer to establish leadership, provided an introduction to CIT's 2003 White Paper entitled "A Proposal to Establish the Virginia Nanomanufacturing Initiative," offered an overview of the competitive landscape of nanotechnology, and updated the Advisory Committee on Nanomanufacturing Initiative progress.

The Commonwealth must be able to answer several questions to establish itself as a leader in nanotechnology. It must review the opportunities that exist, understand the competitive landscape, and identify the influencing factors on development. Furthermore, it must decide whether leadership requires public sector involvement, and if so, whether this involvement includes the federal, state, or local levels of government. Finally, it must determine the steps it should take and when, be cognizant of the consequences of inaction, and review the benefits of strategic actions.

Nanotechnology is the next scientific and industrial revolution. It will play a key role in defense, homeland security, health care, information technology, transportation, and civil infrastructure. John Marburger, Director of the White House Office of Science and Technology Policy, has identified investments in nanoscale science and technology development as essential to winning the war on terrorism, securing the homeland, and strengthening the economy. Experts estimate that by 2015, the world market in nanotechnology will be $1 trillion, and that it will create 800,000 to 900,000 jobs in the United States, with 50,000 jobs in the Commonwealth. Currently, the public and private sectors are investing an estimated $8.6 billion in research worldwide.

The nanotechnology economy brings with it several challenges. First, it requires the ability to manufacture nanomaterials in sufficient volumes and at affordable prices. Second, it requires developing a trained nanomanufacturing workforce. These two challenges illustrate the current missing link in nanomanufacturing: the stage between research and commercial application.

Virginia already has extensive nanotechnology capabilities, including modeling and simulation, nanomaterials design and fabrication, electronically functional materials, carbonaceous materials, emerging technologies like fuel cells and quantum computing, nanobiomedicine, and nanomagnetics. In addition, Virginia's academic institutions are valuable assets, including several four-year colleges and research institutions, the Virginia Community College System, and its primary and secondary education system in grades K through 12. Examples of some of the work currently being performed in Virginia include Luna Innovations' nanomanufacturing facility in Danville, the development of fullerenes (large carbon-cage molecules; a fullerene cage is about 7-15 angstroms in diameter (that's around a billionth of a meter, or 6-10 times the diameter of a typical atom) known as Trimetaspheres at Virginia Tech, research using nanoparticles in neurosurgery at Virginia Commonwealth University and University of Virginia, and biochip research at Virginia Commonwealth University, University of Virginia, and Virginia State University.

In reviewing the competitive landscape of nanotechnology, the presenters shared that leadership in this field is up for grabs among the European Union, Japan and the United States. The United States provided $774 million in government research investments in 2003, compared with $650 in Western Europe and $800 in Japan. In addition, more than 30 countries have national nano activities and Japan currently is focusing on product development. Private venture capital firms also have invested $325 million in nanotechnology in 2003. The hubs of this investment tend to be in Silicon Valley, Boston and Texas. The top five start-up companies -- three in California, one in Texas, and one in Japan -- received about 22 percent of this venture capital. The private money is being invested in electronics and semiconductors (41 percent), nanobiotechnology (40 percent), specialty chemicals and nanomaterials (14 percent), and capital equipment and instrumentation (five percent), all areas of strength for Virginia.

In 2003, Virginia received over $20 million in NSF-supported NNI Research Awards, placing the Commonwealth tenth among states with this type of active support. California was first, receiving about $100 million. New York, Massachusetts Pennsylvania, Illinois, Texas, Wisconsin, Ohio and North Carolina round out the top ten. Between 1976 and 2004, Virginia received approximately 100 nano patents, in comparison to nearly 1300 in California. Currently, Virginia ranks 21st in the number of nanotechnology companies in the states. California ranks first in all categories.

There are currently 23 nanotechnology initiative and development centers in the United States, including the Virginia Nano Initiative. Other states have invested heavily in nanotechnology, including a commitment of $5 million per year for 20 years by Arizona for a Nano-bio research center. California has committed $100 million over four years for the California Nanosystems Institute. Illinois has committed $63 million to the Nanoscience Centers (a university collaboration). New York committed $50 million and $400 million over five yrs to the Nanoelectronics Center. Oregon committed $20 million over five years to the Oregon Nano-Micro Interface Institute. Pennsylvania and Texas have also made substantial state investments. The model for the investments ranges from university-state partnerships to corporate ventures.

To attain leadership, Virginia's mission must focus on the cost-effective manufacture of nanomaterials. The Commonwealth can reach this mission by building a foundation of collaborative research, a users network, and workforce development. The presenters recommended a research investment plan that includes a five-year, $140 million dollar investment model, including $40 million in year one for equipment, research and development, and workforce training, and $25 million per year during the remaining years.

In summary, Virginia can be a leader in nanomanufacturing. Success will lead to the creation of jobs and companies. However, the Commonwealth's role in this development is vital in providing seed funding and facilitating collaboration. However, time is of the essence for the emerging competitive national and international landscape.

Dr. Dylla argued that the report does not answer questions about the long-term return on investment and the short-term leveraged return for investments in nanotechnology. The Committee noted that the Commonwealth has already made substantial investments through the

Center for Innovative Technology (CIT), the Virginia Economic Development Partnership (VEDP) and the educational institutions. According to the VEDP, companies want to know what the Commonwealth is doing in nanotechnology. Dr. Mattauch answered that question by reminding the Committee of the presence of venture capital and university research and technology transfer. He cautioned that the Commonwealth must beware of old research with a new name and avoid the trap of research for research sake. Whatever is developed must be commercializable to be worth the investment. He stressed that researchers must determine the industrial need and potential for their research and that Commonwealth must offer a highly skilled and ready workforce, a welcoming tax and incentive structure and a supportive legal structure to foster the necessary environment.

Nanotechnology Accelerated Development Center

Bruce Swenson, founder and co-Chair of the Northern Virginia Technology Council's Nanotechnology Committee briefed the Committee on a proposed Nanotechnology Accelerated Development Center (NADC) that would focus on prototyping. Of the three pillars of the nanotechnology ecosystem -- research, commercialization, and manufacturing -- the proposed NADC would focus on commercialization, the current weak link in the development of nanomanufacturing initiatives between the research lab and the marketplace. Commercialization involves converting research into a marketable, cost effective product. NADC would provide a physical lab and office facility, foster virtual networks and relationships, assist in developing a trained workforce, and provide demonstrations of nanotechnology capabilities.

The federal Nanotechnology Research and Development Act (S. 189) authorizes approximately $3.7 billion in funding over four years for research and development. Its goals include ensuring the position of the United States as a global leader in the development and application of nanotechnology, and accelerating the deployment and application of nanotechnology in the private sector, including start-up companies. The Act heavily emphasizes research and recognizes that development and commercialization are crucial next steps.

Twenty-one states have 48 nanoscience or nanotechnology initiatives and centers planned or underway. Thirty-three of these centers are university-based, five are in national laboratories, and 10 are state or city programs. A few states, such as New York, Oregon, and Texas have very robust initiatives underway. In addition, Department of Defense Initiatives are underway at the service, laboratory, and program levels. These initiatives have a strong emphasis on fundamental research, but little focus on customer needs, program requirements and possible nanotechnology solutions. Involvement with industry is typically indirect through partnerships with specific research centers or area initiatives.

A gap exists in transitioning basic research to a commercial market. Small businesses often lack the expertise and resources to transition basic research to the commercial market, while large businesses view nanotechnology as too high a risk. This gap complicates the development of nanotechnology products. As research transitions to the marketplace, the technology undergoes several evaluations and validations. Researchers initially create a proof of concept and validate it in the laboratory environment. Then, they must validate that concept as being relevant outside of the laboratory environment, and develop prototypes to show function in an operational

environment. Until they can demonstrate that a product functional relevance, investors will consider any investments high-risk.

A federal and Commonwealth government-seeded prototyping center would bridge this commercialization gap, by assisting in the transition of research into an operational product. Goals of the NADC would be to create an industry-run center, support prototyping and accelerated development of nanotechnology, transition basic nanotechnology research to commercial markets, focus on industry and government needs in project development, and integrate with and support Virginia's nanotechnology research, development and manufacturing activities and resources. NADC would address basic research and customer needs to assist in developing a product useful to commercial and government markets.

NADC would lead to the development of innovative technologies, and would provide partners willing to assume a portion of the project risk. The Center would provide a venue to showcase Virginia nanotechnology research and development and potential applications. The intent of NADC is to achieve a threshold of credibility for innovations, with an emphasis on deliverables that reduces the risk for industry and government sponsors. NADC would also emphasize business development, with a focus on internships and training. The creation of new nanotechnology product lines would create in the Commonwealth and the nation.

Such a center would help to establish the Commonwealth's role across the full life-cycle of nanotechnology and would leverage investment in basic research and development. The center would make prototyping and demonstration capabilities available to the Department of Homeland Security, the Department of Defense, other government agencies, industry and academia.

A prototyping facility would provide instrumentation, staff and space in a facility in the Northern Virginia area. This location already is a hub for industry and corporate offices and leverages access to government agencies and markets. The facility would have the ability to work virtually with other research and development facilities, and could serve as a model for other facilities around the country while establishing Virginia as a leader in nanotechnology.

The goal of NADC is to supplement the costs of the prototyping phase of development, and not the full life-cycle of the nanoproduct. In prioritizing a project, there must be an industry or government transition manager, and the project must have the capability to meet specific industry or government requirements. There must be an assessed return on investment and jobs from the follow-on product line. The estimated budget of such a center would include $20 to $30 million for infrastructure and $25 million annually to provide projects with $1 to 2 million per project for two to three years of funding.

Mr. Swenson concluded by arguing that the Nanotechnology Accelerated Development Center provides a mechanism to transition basic nanotechnology research to government and commercial markets. Furthermore, it allows and encourages a more prominent role of industry in the development and commercialization of nanotechnology. More importantly, it maintains the U.S. leadership and establishes Virginia leadership in the full life-cycle of nanotechnology --

research, development, prototyping, manufacturing, and commercialization -- defining the essence of a "The Nano-Commonwealth."

Such ventures are already underway and can draw and create opportunities. Mr. Smith warned that SUNY-Albany already has a prototyping facility and it does attract business opportunities. Dr. Mattauch warned that such a facility needs to demonstrate an impact and explained VCU's new initiative to achieve a multi-disciplinary program that combines the ability to visualize, create on a computer and produce a prototype with the precision of one-half of one-thousandth of an inch at a time.

Federal Initiatives

Dr. James Kadtke, Science Advisor for United States Senator John Warner, led a discussion of federal initiatives and general issues surrounding the advancement of nanotechnology in the Commonwealth. He began his career as a physicist for the University of California - San Diego before moving to a technology company that evaluated defense technology. Dr. Kadtke joined the government as part of the Science and Technology Policy Institute at the White House, and then worked with a Committee of the House of Representatives before joining Senator Warner's Office. He has a background in identifying economically viable technology. His presentation fostered a great deal of discussion amongst the Committee as to nanotechnology needs in the Commonwealth.

Nanotechnology is revolutionary and has the potential of transforming society by generating new classes of products. It involves manipulating atomic structures to create new materials with new properties. Scientists build these materials from the bottom up and not the top down, as in other disciplines. Experts project that this market will reach $1 trillion in 10 to 15 years. However, job growth is a current problem, as there is no assured process to generate jobs in the industry.

Attempts to coordinate federal work on the nanoscale began in November 1996, when staff members from several agencies decided to meet regularly to discuss their plans and programs in nanoscale science and technology. The group produced two relevant background publications in late 1999: "Nanostructure Science and Technology: A Worldwide Study," a report based on the findings of an expert panel that visited nanoscale science and technology laboratories around the world; and "Nanotechnology Research Directions," a workshop report with input from academic, private sector, and government participants. These documents laid the groundwork and provided the justification for seeking to raise nanoscale science and technology to the level of a national initiative. Subsequently, in its 2001 budget submission to Congress, the Clinton administration raised nanoscale science and technology to the level of a federal initiative, officially referring to it as the National Nanotechnology Initiative (NNI).

After the government established the NNI, it established the Nanoscale Science, Engineering and Technology Subcommittee and gave it the responsibility for coordinating the federal government's nanoscale research and development programs. The Subcommittee is a component of the National Science and Technology Council's (NSTC) Committee on Technology, which is composed of senior-level representatives from the federal government's

research and development departments and agencies. It provides policy leadership and budget guidance for this and other multi-agency technology programs.

The National Nanotechnology Coordination Office, which was established to serve as the secretariat for the Subcommittee, serves as the point of contact on federal nanotechnology activities for government organizations, academia, industry, professional societies, foreign organizations, and others. It maintains the NNI website (www.nano.gov). Over the years, NNI has grown from five agencies coordinating their activities to 15. Currently, 12 state and regional nanotechnology initiatives also work with the National Coordinator providing seed money for infrastructure.

Foreigners are gaining on the United States in terms of education. Fewer Americans are training in science and technology and fewer foreigners are staying. Whereas foreigners used to remain in the United States, now, they are taking their education and going home for opportunities. One member noted that even the President of U.C.-Berkeley resigned and moved to Taiwan to work on their initiatives.

Taiwan is a remarkable example of what countries can do in such a short period of time. In seven years, Taiwan transitioned from an agrarian to a technology economy. It adopted a cluster model and created clusters of development and growth in four cities with the largest bringing in $20 billion. Each of these cities has over 200,000 scientists most of whom were trained in the U.S. While U.S. degrees are highly valued, both China and Taiwan has taken the educational expertise developed by its citizens in the United States and used it to build their own homegrown institutions to train new graduates.

The United States in not sitting still. In the defense bill for fiscal year 2005, Congress designated $2 million for a Virginia-based pilot project with the Navy to promote science and technology among students. Small grants of $1,500 to $2,000 will entice high school students to work in a national lab in Virginia during the summer. If successful, this program could expand into a national program. The cost per student is relatively low, but private sector matching grants could become available if the program is successful. In addition, Senator Warner introduced the 21st Century Federal Pell Grant Plus Act (S. 2462) to double the amount available for those students who pursue programs of study in engineering, mathematics, science, or foreign languages. Congress has not acted on the bill. The programs, and money for them, do exist; however, they are critically underfunded.

Elements to Attracting Industry

Dr. Kadtke's remarks sparked a lengthy discussion amongst the Committee members concerning the importance of education in nanotechnology development. Dr. Kadtke noted that the development stage -- between research and commercialization -- is the piece that the United States is currently missing. He characterized this as the "engineering side," and indicated that intellectual property development is currently moving offshore. He explained that the Koreans, Japanese and Taiwanese now fear the Chinese who are training engineers to transition intellectual property into products.

The educational issue goes deeper than just engineering and intellectual property conversion, and affects the technical workforce as well. The Commonwealth needs a formal sub-B.S. education program that includes K through 12, community college programs and technology school training. The lack of such a comprehensive education system deters foreign investment.

Penn State University (PSU) and the Pennsylvania Community College System (PCCS) developed such a program that combines their expertise to train a nanotechnology-skilled workforce. Students study for two years at a community college and two years at PSU before moving on to a Master's or Ph.D. program. The program consists of two large buildings filled with laboratories and equipment. They collaborated with the private sector, which provided the equipment for this program. PSU and PCCS needed the equipment and the companies need a trained workforce.

Another key issue is how to interest younger people in nanotechnology. Outreach initiatives such as demonstrating that nanotechnology is a legitimate and exciting career path, is the only way to being attracting younger people. Even if students are interested in nanotechnology at the K-12 level, they will not continue at the community college and undergraduate level if the incentives are not apparent to them. Dr. Varshney from the National Science Foundation (NSF) explained that NSF has a program that places high school teachers in a nanotechnology center for three months during the summer for training; they incorporate what they learned in their class teachings during the school year. Members of the Committee suggested that the Commonwealth needs to tap into those funds. NSF currently offers about $40 million to promote K-12 teaching in nanotechnology and other sciences. For such programs to be successful, however, the education system must emphasize higher math and sciences at a young age.

One member reminded the Committee that kids used to learn about science by fixing cars and farm equipment. With this method quickly declining, another one needs to replace it. In addition to showing kids a career path, an opportunity for hands-on experience must exist. Given the cost of advanced education, they must also have the ability to work and gain experience while working toward a degree.

Other members noted that while education is important, it presents a "chicken and egg" issue. Students must see that jobs exist to encourage them to study in this area; however, businesses want to see an educated workforce in a locale before they will locate there. Seed money could be one way to solve this problem. There are generally two approaches to this problem -- a top down approach that would involve bringing in big companies, and a bottom up approach, focusing more on encouraging small start-up companies. Luna Industries in Danville created a business model around using research and intellectual property from universities, and building a facility around that need. For this model to be successful, policy and tax incentives must be in place. In that case, federal, state, and local government as well as the universities worked together.

One member suggested a way to train people without having the necessary industry in place by training people in industries with like technologies. The Commonwealth could use this trained workforce to attract nanotechnology-based businesses. Once businesses establish themselves in the Commonwealth, these trained workers easily could migrate to those businesses.

Conclusions

The Committee concluded by discussing the wide range of possible actions that could encourage nanotechnology development, ranging from seed money and tax incentives to educational and technology transfer efforts. While the Committee made no formal recommendations, there was general consensus that discussion in this area must continue. The Committee was generally in favor of having a more permanent group to foster communication and the exchange of ideas.

Delegate Purkey thanked the members for sharing their expertise on this important issue. While JCOTS formed this one-year study committee as a result of HJ 120 (2004), he wrote a letter to the Speaker of the House and Chairman of JCOTS urging them to continue this Advisory Committee as a resource, and to advise the General Assembly on the next steps in this area.

D. PRIVACY

- **Delegate May, Senator Watkins, and Delegate Alexander co-chairs**

The Advisory Committee on Privacy met four times during the 2004 interim: on July 7, August 18, October 6 and November 17. During its meetings, the committee received briefings on event data recorders, radio frequency identification, tracking technologies for 911, spyware and facial recognition technology, the use of biometrics for identification, and personal information in court records. The Committee also reviewed and discussion selected privacy-oriented bills from the 2004 Session as well as current legislative proposals.

Potentially Invasive Technologies
House Bill 1304 (Lingamfelter)

During the 2004 Regular Session, the House Committee on Science and Technology (HCST) considered and carried over bills that would have required (i) public bodies to conduct a privacy impact analysis when authorizing or prohibiting the use of invasive technologies and (ii) manufacturers of vehicles equipped with recording devices to disclose that fact in the owner's manual. HCST referred these bills to JCOTS for study.

Delegate L. Scott Lingamfelter (House Bill 1304) explained that HB 1304 would have required public bodies to conduct a privacy impact analysis when authorizing or prohibiting the use of invasive technologies, such as radio frequency identification, tracking systems, facial recognition systems, hidden cameras, spyware, photo monitoring systems, and Internet wiretaps beginning July 1, 2006. The bill also would have required JCOTS to propose to the Governor and the General Assembly policies and guidelines for public bodies to follow in conducting the privacy impact analysis. In developing the policies and guidelines, the bill required JCOTS to review the invasive technologies available for use, the current legal requirements of their use and the reasons for their use, their impact on civil liberties, and any safeguards that are or should be used to mitigate negative impacts.

Delegate Lingamfelter said that he introduced the bill because he realized that while the legislature has been asked to authorize, limit or prohibit the use of many new technologies such as facial recognition and photo monitoring systems, the needs of legitimate law enforcement must be balanced against the preservation of the American way of life and inalienable freedoms. He understood that the development of new technologies has challenged the balance between civil liberties and security, a long-established principle embedded in the constitutions of the United States and the Commonwealth of Virginia. Technologies available today can track a person's movement, listen to his conversations, assess the speed of his vehicle and look inside his house all from a remote location and without his knowledge. As they become more invasive and their use more clandestine, the potential for unchecked abuse threatens to impinge civil liberties. Therefore, Del. Lingamfelter found it crucial to have more information when deciding on legislation that affects their use.

Event Data Recorders
House Bill 697 (Morgan)

On behalf of Delegate Harvey Morgan (House Bill 697), staff briefed the Committee on HB 697, which would have required a manufacturer of a new motor vehicle sold or leased in the Commonwealth that is equipped with one or more recording devices, commonly referred to as "event data recorders" (EDR) or "sensing and diagnostic modules" (SDM), to disclose that fact in the owner's manual for the vehicle. The bill would have prohibited specified data that is recorded on one of these devices from being downloaded or otherwise retrieved by a person other than the registered owner of the motor vehicle, except under specified circumstances. The bill also would have required a subscription service agreement to disclose that specified information may be recorded or transmitted as part of the subscription service.

Robert J. Breitenbach, Director, Transportation Safety Training Center, Virginia Commonwealth University, provided an overview of the history and use of EDRs. On June 10, 1997, the National Transportation Safety Board (NTSB) adopted a series of new recommendations on air bags and automobile occupant restraint use. The recommendations arose from the NTSB's public forum convened in March 1997. One of the recommendations the NTSB made to the National Highway Traffic Safety Administration was to "develop and implement, in conjunction with the domestic and international automobile manufacturers, a plan to gather better information on crash pulses and other crash parameters in actual crashes, utilizing current or augmented crash sensing and recording devices." In response to this recommendation, domestic automobile manufacturers began introducing "EDR" functionality in its current form in vehicles for model year 1997. However, EDRs were first introduced in model year 1990 vehicles that were equipped with air bags and only recorded very limited data.

EDRs made by different manufacturers record different data. However, most EDRs record whether the driver's and passenger's seat beats were buckled or unbuckled, whether the air bag engaged, engine speed, vehicle speed, and whether the brake switch was on or off. The devices begin recording vehicle data when the device detects the vehicle slowing down along its length with enough force to cause the module's crash sensing algorithm to 'wake up' and anticipate a collision severity which warrants an actual deployment for that vehicle. Technicians can download information from the devices either using the vehicle's diagnostic link connector

(DLC), which is installed under the dashboard on all vehicles from 1996 or later or directly from the air bag module located under the passenger's front seat.

Mr. Breitenbach illustrated six sets of crash data for the Committee, using each set to highlight different aspects of EDR data as it is used in analyzing automobile crashes. In addition to the data collected by EDRs, crash reconstructionists collect and analyze real world data, such as acceleration/distance analysis and speed determination. The real world data is often gleaned from physical evidence, including skid marks and a thorough examination of the crash site and the automobiles involved. In each set of crash data, the data recorded by the EDR was generally consistent with the physical evidence observed and the reconstruction analysis. Some crash situations may make the EDR data inconsistent with physical evidence, such as when a vehicle goes airborne or a wheel breaks from its axle. In these cases if the accelerator is continuously applied there may be spikes in engine speed and vehicle speed.

Mr. Breitenbach emphasized that the EDR is a tool to be used by the crash reconstructionist, not a replacement for them. The device supplements good investigative and analytical procedures. It does not stand alone in many real world events; a full analysis of the crash is still required.

In spite of the value of the data recorded by EDRs, significant privacy concerns surround these devices. Most notably, EDR data is relatively easy to retrieve, requiring only a small investment in hardware (several thousand dollars at most), working knowledge of the software, and access to a vehicle containing an EDR. The information, while gathered to enhance safety in motor vehicles, can be used to determine fault in the event of a crash, whether the driver wore a seat belt and potentially even driving habits.

Information Collected by Event Data Recorders

On behalf of the Alliance of Automobile Manufacturers (AAM), James Beamer briefed the Committee on the use of event data recorders and similar devices in transportation and the use of information collected.

Aviation was the first mode of transportation to use data recorders in the late 1950s. Marine followed roughly two decades later. Not until the late 1980s were these devices used in passenger vehicles and then only on heavy vehicles. Light vehicles followed in the mid 1990s as did railway. Over the years, federal government agencies, such as the National Transportation Safety Board (NTSB), National Highway Transportation Safety Administration (NHTSA) and NASA Jet Propulsion Lab, have recommended their use to gather and analyze crash data. NHTSA has since proposed a regulation calling for recording a minimum set of specified data elements, specifying requirements for data format, requiring vehicle manufacturers to make publicly available information for accessing EDR data, increased survivability requirements, and a standardized owner's manual disclosure statement.

Not to confuse the capability of EDRs, Mr. Beamer distinguished them from flight data recorders (FDRs). Unlike FDRs, EDRs provide an understanding of vehicle system operations as opposed to accident reconstruction and record limited data for a limited period without audio and under very limited circumstances. Understanding that even collecting this limited data raises privacy

concerns, AAM advocates that access to EDR data be limited only (i) to those with the consent of the vehicle owner or lessee, (ii) in litigation through the discovery process, (iii) in response to an official request of police or similar government office, or (iv) as otherwise required by law.

Other Devices

Adding to the debate, staff informed the Committee of additional devices that companies are installing in vehicles and the expanded purposes. While manufacturers install EDRs, which record limited information for a limited period, at the factory, other devices are not so limited. On August 12, 2004, the Wall Street Journal reported that Progressive Corporation was beginning a pilot program in Minnesota to track how often, how far and how fast people drive. In exchange for reduced rates, the insurer would provide as many as 5,000 volunteers with a matchbox-sized electronic device to be installed in their cars to gather this information. Progressive has stated that it does not plan to share the information with others and will allow drivers to view their information before deciding whether to submit it. This action raises the questions: who owns the information and who can access it.

With gas-tax collections declining as fuel efficiency increases, some states are researching how to replace the fuel tax with a fee based on the number of miles traveled. Fees would be measured by Global Positioning Systems receivers embedded in vehicles. The system would track which roads a motorist uses so the "virtual tolls" could be distributed to the appropriate agency.

Companies with truck fleets are using even more sophisticated devices. Engineers use them to determine truck performance for providing effective maintenance and building better trucks. Fleet operators use them to determine how their trucks are driven and what their drivers are doing. The information provided by these devices can help companies that depend on trucking, such as shipping companies, to track packages, trucks and mileage driven, thus providing them with opportunities to make their operations more efficient and reduce costs. The uses are endless, but the issues are the same.

Radio Frequency Identification

Bradley Canel, Manager, Accenture Technology Labs, briefed the Committee on radio frequency identification (RFID). RFID is a generic term for technologies that use radio waves to automatically identify people or objects. RFID uses several methods of identification, but the most common is storing a serial number that identifies a person or object, and perhaps other information, on a microchip that is attached to an antenna (the chip and the antenna together are called an RFID transponder or an RFID tag). The antenna enables the chip to transmit the identification information to a reader. The reader then converts the radio waves reflected back from the RFID tag into digital information that can then be passed on to computers that can make use of it.

An RFID system consists of a tag, which consists of a microchip with an antenna, and an interrogator or reader with an antenna. The reader sends out electromagnetic waves. The tag antenna is tuned to receive these waves. A passive RFID tag draws power from the field created

by the reader and uses it to power the microchip's circuits. The chip then modulates the waves that the tag sends back to the reader and the reader converts the new waves into digital data. Active RFID tags have a battery, which runs the microchip's circuitry to broadcast a signal to a reader (the way a cell phone transmits signals to a base station). Passive tags have no battery. Active and semi-passive tags are useful for tracking high-value goods that need to be scanned over long ranges, such as railway cars on a track. They cost a dollar or more each, making them too expensive to put on low-cost items. Companies are focusing on passive tags, which cost approximately 25 cents each when purchased in volumes of 1 million tags or more. Their read range is not as far -- typically less than 20 feet as opposed to 100 feet or more for active tags -- but they are far less expensive than active tags and can be disposed of with the product packaging. Passive tags have considerable benefits, particularly in retail inventory applications.

RFID tags differ from the traditional bar code technology because they do not require line of sight. They can be read as long as they are within range of a reader. Bar code scanners must be near a scanner that can "see" the bar code to read it, which means people usually have to orient the bar code towards a scanner for it to be read. If a bar code label is ripped, soiled or falls off, there is no way to scan the item. RFID codes are long enough that every RFID tag may have a unique code, while UPC codes are limited to a single code for all instances of a particular product. The uniqueness of RFID tags means that a product may be individually tracked as it moves down the supply chain. This may help companies to combat theft and other forms of product loss. RFID tags enabling everything from tracking cows and pets to triggering equipment down oil wells. The most common applications are tracking goods in the supply chain, reusable containers, high value tools and other assets, and parts moving to a manufacturing production line. RFID is also used for security (including controlling access to buildings and networks) and payment systems that let customers pay for items without using cash.

The use of RFID technology has generated considerable controversy and even product boycotts. The four main privacy concerns regarding RFID are (i) the purchaser of an item will not necessarily be aware of the presence of the tag or be able to remove it; (ii) the tag can be read at a distance without the knowledge of the individual; (iii) if a tagged item is paid for by credit card or in conjunction with use of a loyalty card, then it would be possible to tie the unique ID of that item to the identity of the purchaser; and (iv) tags create, or are proposed to create, globally unique serial numbers for all products, even though this creates privacy problems and is completely unnecessary for most applications.

Most concerns revolve around the fact that RFID tags affixed to products remain functional even after the products have been purchased and taken home, and thus can be used for surveillance, and other purposes unrelated to their supply chain inventory functions. Although RFID tags are only officially intended for short-distance use, they can be interrogated from greater distances by anyone with a high-gain antenna, potentially allowing the contents of a house to be scanned at a distance. Even short range scanning is a concern if all the items detected are logged in a database every time a person passes a reader, or if it is done for nefarious reasons (e.g., a mugger using a hand-held scanner to obtain an instant assessment of the wealth of potential victims). With permanent RFID serial numbers, an item leaks unexpected information about a person even

after disposal; for example, items that are resold, or given away, enable mapping of a person's social network.

Mr. Canel emphasized that radio frequency technology by itself is not invasive, but how the technology is employed to track objects may be. When asked whether an RFID tag embedded in a garment that is stolen could be read when the garment is worn into another RFID-enabled area, he replied that the present state of radio frequency technology does not permit ubiquitous radio frequency reading. He encouraged the Committee to keep three considerations in mind when addressing RFID issues: (1) the range at which the RFID tag can be read, (2) the purpose for which the RFID tag is being used, and (3) how access to and control of the information contained in the RFID tag will be managed.

Tracking Technologies for 9-1-1

Steve Marzolf, Public Safety Communications Coordinator, Virginia Information Technologies Agency, explained the tracking technologies used by the Commonwealth to help locate 9-1-1 callers whether from wireline or wireless phones. Wireline phones provide the registered name, physical address, telephone number, and class of service (residential, business, etc.) for all callers to 9-1-1 operators. The call center can manually look-up this information by telephone number, if necessary. Additionally, information is available for exigent circumstances even if 9-1-1 not called.

Wireless phones provide two phases of information for callers to 9-1-1. Phase I provides a call back number and the address of the cell site processing the call. Phase II provides the Phase I data as well as the longitude and latitude for the caller with the accuracy being dependent on the technology. The accuracy of the Phase II location data can be addressed either through a handset-based solution or a network-based solution. The handset-based solution requires a global positioning system (GPS) in each handset; older handsets would have to be replaced and activated. This technology can provide an accurate location to within 50 meters of the phone on 67 percent of the calls, and 150 meters on 95 percent of the calls. The network-based solution triangulates the phone's location based on at least three cell sites. It works with existing handsets, but requires involving the carrier of the cell phone's signal. This technology can provide an accurate location to within 100 meters of the phone on 67 percent of the calls and 300 meters on 95 percent of the calls.

In addition to using telephony to locate 9-1-1 callers, 9-1-1 call centers also have access to multiple mapping and geographic information systems (GIS) databases, including digital aerial photography, assessment and property owner data, building photographs and plans and previous incident history. Future technologies may be able to track any type of communications whether through computers (telematics) or voice over Internet protocol (VoIP). Telematics may provide transmission of collision data to 9-1-1 center from an EDR, which would potentially assist emergency workers in determining an appropriate level of response. VoIP is an increasingly popular means of telephone service; however, 9-1-1 call centers receiving such a call need the ability to track the caller's location via the Internet and then route the call to the appropriate 9-1-1 center.

Use of this data is governed by the Wireless Communications and Public Safety Act of 1999 (WCPSA - 47 U.S.C. § 222) and the Communications Assistance for Law Enforcement Act of 1994 (CALEA). The WCPSA protects subscriber and location information and provides an exception "solely for purposes of assisting in the delivery of emergency services in response to an emergency." This law allows access to subscriber information for emergency notification systems. CALEA requires a court order for other subscriber and location information. All 9-1-1 lines are recorded, and those recordings are public information subject to freedom of information laws.

Spyware

Spyware refers to executable programs placed on a computer, usually without permission or knowledge, that monitor or access information and report it to a third party. The programs can record keystrokes, take screen shots, scan files, install other programs, or monitor systems, providing access to passwords, credit cards numbers, and other sensitive information -- and even the ability to control the computer -- all without the user's knowledge, even if the user is not connected to the Internet.

Spyware can compromise critical information, lead to loss of intellectual property or other competitive advantage, and cause compliance issues as governments pass stringent laws to protect medical, financial and other sensitive data. They can violate privacy, detract from the computer's usability and stability, appropriate resources and even alter functionality.

A computer user can acquire spyware by clicking on deceptive pop-ups or links in e-mail, visiting certain websites that may require a plug-in, as a piggyback to a download or any number of other ways. Sometimes, the user unknowingly gives permission to receive the spyware by agreeing to, though not necessarily reading, a lengthy end user license agreement while downloading software.

Commonly-used security measures have proved inadequate to stop these programs. Firewalls operate on the boundary of networks and cannot detect spyware that is introduced from or is already running within the network. Anti-virus software typically does not detect spyware. Not even encryption can stop it because keystroke loggers record keystrokes before the information ever is encrypted.

Software companies have developed programs to detect, disable, intercept or remove spyware, though they are of limited value. Some spyware vendors use techniques to avoid detection and removal, such as counterattacking the software in an attempt to disable it. Other programs use routines to re-install themselves after detection and deletion, or can defeat attempts to cut off their communication.

The best ways to stop spyware is to stop (or stop employees from) visiting websites known to distribute it and downloading applications that are infected with it. Computer users can install and operate intrusion detection software to alert them if anyone is trying to hack into their systems or send information through the Internet. Finally, setting the Web browser's security level to high and monitoring for and installing updates and security patches will better protect

computer users. If all else fails, users must back up data in case their files are corrupted or destroyed.

Brian Tretick, Technology and Security Risk Services, Ernst & Young, briefed the Committee on spyware. The term "spy" is misleading because even some of the most annoying software does not actually send any information back to a server or another third party, though it does retrieve information. Computer security people tend to call it all "malware," meaning it is harmful software. Some people distinguish "adware" (advertising-supported software that displays pop-up advertisements whenever the program is running) from "real spyware," such as Trojan horses (a destructive program that masquerades as a benign application) and keyloggers (programs that record every keystroke and transmit the information to a third party). Typically, spyware arrives bundled with freeware or shareware, through email or instant message, or by someone with access to a user's computer.

It is often easier to define the bad things that should be avoided, rather than all the good things that should be allowed. Some of the bad things occurring today include software acting in unfair or deceptive ways, such as hijacking the computer or network resources; modifying the computer, network or other software or their configurations; and snooping, capturing data, or otherwise surveilling the computer, network, or other software. This includes use of email, instant messaging, Internet browsing, and even word processors. However, legitimate software may operate and have functions that the user is unaware of. Some current practices include targeting ads in exchange for some other benefit, such as special offers; monitoring and analyzing behavior; troubleshooting, error calculating and error reporting; and grid computing, using idle time to process a larger problem.

To get rid of the "spy" in spyware, industry and legislators must focus on transparency and other control by the user. Software must provide clear, conspicuous and accurate notice to the user; a consent requirement, involving informed consent; and the ability to disable and configure the software. Software should not provide a "silent back channel" communication or ET "phone home" features without notice to and control of the user or collect more information than necessary. Legislation must not eliminate legitimate, ad-supported software.

Facial Recognition Technology

Greg Mullen, Deputy Chief of Police, City of Virginia Beach, briefed the Committee on the City of Virginia Beach's process for implementing facial recognition technology (*see* Appendix 6). Residents throughout the Hampton Roads area and several million tourists visit the Virginia Beach oceanfront. To maintain the Virginia Beach Police Department's commitment to the safety and security of these tourists and residents, the city added facial recognition technology to the existing closed circuit television video camera system during the summer of 2002. Until that point, Tampa was the only other jurisdiction to use it.

Prior to implementing the technology, the Department researched it for several years beginning in 1999. Facial recognition technology is a biometric application that converts an image (e.g., a mug shot or photograph) into a mathematical algorithm that a computer can use to compare that

image to another one. The Department developed a dynamic database of pictures and biographical data on people that meet specific criteria. The cameras scan locations where people frequent attempting to match images of those people with images in the database. Police Department tests of the system, which are conducted annually, show an 84 to 85 percent accuracy rate. Tests during all light conditions, show an accuracy rate in the mid-70 to mid-8-percent range.

Above all else, the Department believed that full disclosure was paramount to implementing a successful program. Using a grant from the Department of Criminal Justice Services, the Department set out to involve the community and let them know that the Department was not trying to hide anything. It initiated a media and communication campaign to disclose what the technology can do, why the Department was implementing it, and how it would be deployed. News releases, media interviews and a city website helped the Department reach out to educate the community by dispelling myths and spreading facts.

After fully disclosing its intentions and conducting the research, the Department began an education campaign, first by briefing city leaders on the potential for using the technology and then by educating the public. The Department briefed the City's Human Rights Commission to learn of issues that might affect citizens and worked with interested groups including civic organizations, business communities, boards and commissions.

To foster public input, the Police Department held a town hall meeting on the technology and streamed the meeting on the Department's website to provide greater access. During this meeting, a panel of experts in privacy, law enforcement, business and research - the President of the Virginia ACLU, a Rand researcher, the Police Chief, a representative from the business community, a representative from the Tampa Business Community Advisory Board, and a civil rights lawyer - answered questions from the public. In addition to televising the meeting, the Department also advertised the issues and answers to the questions on the website and through the local newspaper.

To maximize public knowledge and input, the Department publicized its effort through interviews with local and national television stations, conducted one-on-one briefings with council members to address all the issues and possible problem areas, and held a public hearing with the council prior to a vote. When Council made the decision to implement the system, the Department held a news conference to inform everyone and reinforce its commitment to ensuring that the program was operated in a manner that balanced law enforcement's needs and those of the community. The Department held another new conference once the system was operational and provided demonstrations, allowing the media to film use of the system in process to verify that the Department is doing what it said it would do.

In addition, the Department formed the Facial Recognition Technology Citizen’s Advisory and Audit Committee. Because the Department believed that it was important for the group to reflect the community, it included representatives from the NAACP, Hispanic Dialog, Human Rights Coalition, the local Philipino community, and other human rights and minority groups. The Committee exists to oversee and assist in the preparation and implementation of the policies and procedures that govern the Department’s program.

Together, the Department and the Committee developed specific criteria for the type of people who would be in the database and the policies for operating the system. First, people with outstanding felony warrants (about 650) were loaded into the database. Later, the group added lost or missing children, runaways, other missing persons, the Top 20 Terrorists and the FBI's Top 10 Most Wanted. Finally, law enforcement officials can request that a specific individual be added for a specified, limited time. The database would not store images from the cameras and would be reviewed daily and updated accordingly. To limit privacy concerns, the data would not be stored and the system would not be connected to outside databases or the Internet.

Using an algorithm that contains 80 points of the face, the technology avoids bias and stereotype. The closed circuit television video feed, which is saved for seven days, sends images to the system for comparison. A match creates an alert. The system then sends the image and the top ten closest matches from the database to an officer for comparison. The system only saves the image if the officer verifies the match and prints the image. Then, the Department will dispatch an officer for a voluntary encounter according to its standard operating procedures.

To protect the citizens, the Department must have policies for everyone using the technology. A police officer audits the system monthly and a private citizen group audits it quarterly through random audits to ensure compliance with the policy and maintain the integrity of the system. Civil Rights groups also have uninhibited access to audit the system and report on its progress. The system is not used unless trained officers are present. The Department provided schedules of use to the audit committee so that they can audit it when it is operational.

The Department's use of facial recognition technology is publicized throughout the area with signs warning people and cameras located in plain sight. The Department received a $200,000 grant to purchase and install the equipment, train officers in its use and maintain it for three years. The system replaced the manned surveillance cameras that were typically used during events and holidays. The Department also used cameras to videotape arrests to protect police and suspects. It needed something better and less expensive to identify and prevent problems and deter crimes in the area. The Department enhanced its current infrastructure and built a scaleable system. In the two years that it has been running, there have been no complaints and no arrests. According to Deputy Chief Mullen, the area is one of the safest in the Commonwealth and his Department wants it to stay that way.

After the presentation and questions, the Committee discussed other uses of such a system. Currently, Arizona and Florida are using this technology at their Department of Motor Vehicles Offices and jails. In addition, they connected their system more systems than Virginia Beach. Senator Watkins cautioned that private entities can take photographs without most privacy issues and at some point, run them through this type of system. Deputy Chief Mullen responded that the Las Vegas casinos do this now. He reminded the Committee that facial recognition technology is just another tool to increase the chance for apprehending wanted people, deterring crime and saving runaways. Even a 50 percent chance (the Department of Defense accuracy rate) is better than no chance at all.

Identification Documents, Biometrics and the Commonwealth

Karen Chappell, Deputy Commissioner for Operations, Department of Motor Vehicles (DMV), discussed the use of biometric technologies to verify identity at DMV. DMV is seeking a legislative study on the use of biometrics for state agencies. It had planned to develop a legislative proposal seeking the authority to collect and use biometrics on the Commonwealth's driver's license and ID card issuance process.

However, recognizing that the capture and storage of biometric data is a sensitive issue, DMV decided that an impartial group should conduct a study on the use of this technology for all agencies that may benefit from it (e.g., State Police, Social Services, and the Department of Medical Assistance Services). Such a study group would need to evaluate the reliability of available technology, implementation costs, and the potential privacy impact, among other critical issues.

Because state-issued driver's licenses and ID cards have become the primary method of identification, DMV believes that the Commonwealth must take every possible action to strengthen the issuance process and the integrity of the documents. The agency believes that using biometrics will help it reduce fraud and improve efficiency in the issuance process.

In a driver's license process, biometrics can function in two ways--- as identification and verification. As identification, the agency would use an applicant's unique identifier information to search an existing database for duplicate data, a one-to-many search. Such a search would help the DMV customer service representative confirm, before issuing the driver's license or ID card, that the customer does not already hold a license or ID. As verification, the information collected could confirm an individual's claimed identity, a one-to-one search, determining that the biometric on file belongs to the cardholder.

Ms. Chappell indicated that DMV is most interested in using facial recognition and finger scans. Facial recognition seems to be the least invasive biometric identifier to collect. DMV could obtain facial feature points from digital photographs already on file for current license and ID card holders. In addition, facial recognition scans would be an efficient and versatile way of addressing identity theft and security issues.

Six states have begun using facial recognition biometrics as a way of using technology to make the license issuance process more secure. West Virginia was the first to implement it in 1997. The District of Columbia, Colorado and Illinois also are using it and Alabama and Kansas are in the process of developing the capability. These states use facial scanning to prevent the issuance of duplicate drivers' or fraudulent credentials. Illinois reports that it found tens of thousands of duplicates with some individuals having as many as a dozen licenses.

While most facial recognition applications prevent the issuance of fraudulent cards, states, such as Texas use fingerprint technology to prevent cards already in circulation from fraudulent use. Only the template created after scanning the fingerprint is stored in a database for verification comparisons. The template could not be used to recreate a fingerprint. Five states, Texas, California, Colorado, Georgia, and Hawaii, require fingerprints. Other states collect fingerprint data on a voluntary basis, including Georgia, Oklahoma, West Virginia and Mississippi.

All states will be using fingerprint technology next year to comply with the federally mandated USA Patriot Act. Effective January 31, 2005, the Act will require individuals applying for a Commercial Driver's License (CDL) with a hazardous materials (HAZMAT) endorsement to provide specific information and submit fingerprints for a background check. The application information will be entered into the agency's host system and transmitted to the American Association of Motor Vehicle Administrators' (AAMVA) Commercial Driver's License Information System (CDLIS). CDLIS enables the Transportation Security Administration (TSA) to retrieve the information and perform name-based checks.

In addition, DMV will send fingerprints to the Virginia State Police, who will forward them to the FBI using its existing digitized fingerprint protocol. The FBI will process the transaction and send results to the TSA. TSA plans to compile and review both the data from CDLIS and the FBI and make a security threat assessment. After its review, TSA will provide DMV with (i) an immediate revocation of the applicant's HAZMAT endorsement, (ii) an initial notification of threat assessment, an indication that they found something that may warrant the refusal or revocation of the endorsement, (iii) a final notification of threat assessment, indicating that the applicant is a possible security threat, or (iv) notification that the applicant poses not threat. Based on the results from TSA, the DMV will either issue a CDL with the hazardous material endorsement or send the applicant notification of TSA's denial.

As the agency implements the federal mandate for CDLs, it plans to evaluate the process and the possibility of expanding it for the entire licensing process. In the meantime, Ms. Chappell informed the Committee that DMV is changing the current process for issuing driver's licenses and ID cards to strengthen the security of Virginia credentials. DMV is replacing over-the-counter issuance with centralized issuance.

Using a centralized process, DMV will accept and review customers' applications and conduct required testing at DMV offices. Applicants meeting identity, legal presence, residency, social security and testing requirements will receive a receipt that serves as temporary authorization to operate a motor vehicle. DMV may include the applicant's photograph and will determine how long receipts are valid. DMV will transmit applicant data to a third party vendor who will produce the driver's licenses and ID cards at a central processing point and mail the cards to the customer. DMV employees would no longer be able to issue licenses or ID cards. Fifteen states--- Alabama, Colorado, California, Kansas, Maine, Massachusetts, Michigan, Minnesota, Montana, New York, Rhode Island, Texas Utah, Washington and Wyoming--- already use a centralized system and are able to provide licenses and ID cards within three to five days. This process is similar to the current online renewal system in Virginia and the process used to issue U.S. passports. As DMV implements the central issuance process, it is planning for the possibility of adding biometrics to verify identity.

Information on Court Records: The Court Clerks' Point of View

On behalf of Virginia Court Clerks Association, Chip Dicks briefed the Committee on the court clerks' view on efforts to limit confidential information on court records. Several committees have studied the issue of limiting access to sensitive data (e.g., social security numbers and

financial account information) on government records. The court clerks play an active role in this debate because an overwhelming majority of the affected documents are created by or filed with courts around the Commonwealth.

Mr. Dicks addressed four points. First, the General Assembly in 2003 enacted § 2.2-3808.2, which prohibits court clerks from posting any document that contains specified identifying information on a court-controlled website (i.e., actual signature, social security number, date of birth, mother's maiden name, financial account numbers, or name and age of any minor child). The provision exempts these documents if the court provides them by subscription through secure remote access. The provisions expire on July 1, 2005. While Mr. Dicks acknowledged that the provisions should be reviewed for possible amendments, such as penalties, he asked that the Committee support extending the sunset.

Second, he addressed the Technology Trust Fund. Pursuant to § 17.1-279, the clerk of each circuit court must assess, in addition to other charges, a fee on each document to be recorded in the deed books, and each judgment to be docketed in the judgment lien docket book. The purpose of the fee is for automating, preserving, maintaining and enhancing court records, and improving public access. Through Senate Bill 241 (Patron - Norment), the 2004 General Assembly increased the fee from $3 to $5 and made the fee permanent (previously, it was to expire on July 1, 2008). Mr. Dicks explained that one of the goals of the bill was to provide a dedicated trust fund to enhance technology and efficiency in the Clerks' offices. The Compensation Board, which administers the fund, estimates the amount available to be $8 million per year.

Third, Mr. Dicks expressed a concern regarding the Freedom of Information Act (FOIA). FOIA includes constitutional officers as public records for purposes of disclosure of public records. He explained that clerks have encountered people requesting the entire court records database pursuant to FOIA. Section 2.2-3704 provides that "except as otherwise specifically provided by law, all public records shall be open to inspection and copying by any citizens of the Commonwealth." He stated that the Court Clerks Association believes the provisions requiring subscription-based secure remote access are "otherwise specifically provided by law" and therefore, such records should be available only through that subscription access.

Referring to the position that a court record is a court record regardless of whether it is electronic or physical, he informed the Committee that the National Center for State Courts (NCSC) treats existing records and new records with personal identifying information differently. Going forward, most people agree that court records should not contain personal identifying information, such as social security numbers. Where state or federal law requires inclusion of that information, a cover sheet could be included to keep the information separate from the portion of the record that would be made available to the public. However, for older records, NCSC recommends treating certain domestic relations documents and others of a sensitive nature as sealed for purposes of electronic access and subject to the provisions of current law for access at the courthouse. Someday, software will render this distinction unnecessary, but until then, the Commonwealth must treat the documents differently.

Finally, Mr. Dicks indicated that the Court Clerks support the Uniform Real Property Electronic Recording Act (URPERA), recommended by the National Conference of Commissioners on Uniform State Laws (NCCUSL). While the Uniform Electronic Transactions Act (UETA) provides for the enforceability of electronic documents, URPERA establishes a framework for recording these documents in the land records. Although UETA provides that the Supreme Court may adopt rules for electronic filing of court records, the clerks believe that URPERA would facilitate the business community's utilization of electronic filing. In addition, the clerks believe that NCCUSL's Uniform Residential Mortgage Satisfaction Act could reduce, if not eliminate, the paperwork associated with certificates of satisfaction.

Legislative Proposals

Building upon its work during previous years and upon the presentations and discussions of this year, the Committee discussed a number of legislative proposals.

1. Display of Social Security Numbers - Private Sector

The House Committee on Science and Technology (HCST) considered and carried over House Bill 753 (May), a JCOTS recommendation, that would have limited the use of social security numbers in the private sector. The bill would have amended the Personal Information Privacy Act to protect the social security number from public display and insecure transmission. The bill would have allowed those who use the number prior to the effective date of the bill to continue using it so long as the use was continuous if the user provided to the number holder an annual disclosure and a cost-free opportunity to discontinue use.

The bill also would have required that insurance plans for state employees assign an identification number that is not a covered employee's social security number. Finally, the bill would have amended the Virginia Consumer Protection Act to prohibit a supplier from using a consumer's social security number when the consumer requests that his driver's license number be used. Current law requires that a supplier only provide an alternate number if the consumer so requests in writing. This bill provides consumers with another option other than providing their social security numbers and writing to the supplier for a new number.

The Committee discussed each provision individually. With no opposition or concern over the restrictions on using a social security number as an identifier for state employee insurance plans and further protections in the Consumer Protection Act, the Committee focused its discussion on the provisions that limited the private sector's use of the social security number.

The proposal originally enumerated six limitations, unless a specific law stated otherwise. The first limitation prohibits anyone from "intentionally communicat[ing] or otherwise mak[ing] available, in any manner, an individual's social security number to the general public." The Committee was not satisfied with the practical effect of "otherwise make available, in any manner" and expressed concern that the proposal contained no definition. Members raised questions about whether dropping a document with a social security number on it or posting it in an office was considered otherwise making it available to the general public. One person expressed concern that this provision would prohibit a specific group's otherwise legitimate uses.

The Committee agreed that general public means the public at large and not a specific subset. Therefore, the Committee only voted to remove "or otherwise make available, in any manner."

The second limitation prevents anyone from "print[ing] an individual's social security number on any card required for the individual to access or receive products or services provided by the person or entity." Without objection, this limitation remained unchanged. When presented with a provision to clarify that no one can bypass this requirement to remove social security numbers from these cards by converting them into a machine-readable format, the Committee voted to adopt that provision as well.

The third limitation prohibits "requir[ing] an individual to transmit his social security number over the Internet unless the connection is secure or the social security number is encrypted." The Committee discussed whether the information technology professionals could define secure and encrypted. Members understood that what constitutes "secure" and "encrypted" would change over time and would be different based on the industry and information. Originally, the Committee voted to retain this provision as the best alternative. However, it reopened the debate at the final meeting. A member suggested changing the limitation to require that anyone who asks for the social security number must protect its confidentiality. Committee members believed that this alternative was not only too broad and indeterminate, but also not subject to interpretation by the technology professionals who would have to implement it. Unable to define "secure" and "encrypted" and unwilling to hold up the rest of the limitations, the Committee eventually voted to delete this provision.

The fourth limitation prohibits "requir[ing] an individual to use his social security number to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the site." One member questioned whether this limitation would prohibit a company from asking for a social security number as part of the signup process for accessing a website. Mr. Goldstein responded that because the company was not requiring the social security number to access the website and reputable companies already require additional authentication information at the point of login, this provision would not prohibit current best practices. This provision remained unchanged.

The fifth limitation prohibits "requir[ing] an individual to disclose or furnish his social security number to access or receive goods or services unless the request or requester [was] subject to a state or federal statute, regulation or rule that governs the use and disclosure of social security numbers and such request or use [was] not prohibited by a state or federal statute, regulation or rule. This provision reaches those entities not covered by current privacy laws or subject to other legal restrictions on the use and disclosure of social security numbers (e.g., grocery stores and video rental outlets). Some corporate representatives questioned whether this provision would prohibit them from using the social security number even in cases required by law. However, each of the corporations was an entity covered either by financial or medical privacy laws. In addition, other laws specifically enable an entity (e.g., a landlord or his representatives) to require a social security number to access goods or services (e.g., an apartment rental); this provision would not affect those entities. The Committee did not want to restrict who could require an individual's social security number to access goods and services. Instead, members indicated that an individual could refuse to do business with that particular company.

The final limitation subjects the private sector to the same standard that the Commonwealth requires of itself. It prohibits "send[ing] or deliver[ing] or caus[ing] to be sent or delivered, any letter, envelope or package that displays a social security number on the face of the mailing envelope or package or from which a social security number is visible, whether on the outside or inside of the mailing envelope or package." At prior meetings, the Committee discussed the provision as originally introduced during the 2004 Session:

> Except as otherwise specifically provided by law, a person shall not print an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. This paragraph does not prohibit the mailing of documents that include social security numbers sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the social security number.

Several states that adopted similar statutes used that version. California and Illinois combined the two provisions.

At prior meetings, several corporate representatives indicated that current privacy laws already address what they can do with personally identifying information. They objected to this provision because it only allows uses that are required by law and many of their uses, while not prohibited, are not required. However, at its final meeting, the Committee decided not to discuss these alternatives and, by default, retained the original provision.

No one raised concerns or objections to the next three provisions (i) allowing for continued use of the social security number subject to certain requirements, (ii) protecting uses required by law and those internal uses that the law does not prohibit, and (iii) giving insurance plans until January 1, 2006 to remove social security numbers from identity cards. Therefore, these provisions remained unchanged. The proposal enables insurance companies to treat new and renewing the members the same and remove the number from all identity cards when the plans renew on January 1. Because the Commonwealth's plan begins on July 1, the proposal gives insurance plans for the Commonwealth until July 1, 2006 to comply with that requirement.

Information database companies and credit reporting agencies raised objections that this proposal applies to public bodies. Public bodies already must comply with many of these restrictions as required by the Government Data Collection and Dissemination Practices Act (§ 2.2-3800 et seq.). The intent of this proposal was to apply best practices already required of the public sector and specific industries of the private sector to all industries of the private sector. Therefore, the Committee voted to add a provision clarifying that this proposal does not apply to public bodies.

In addition, these organizations objected to applying these limitations to public records. They argued that other states that adopted similar statutes exempted public records. However, while some of these states exempted public records, their public records laws differ from the Commonwealth. For example, some states' public records laws exclude social security numbers

from their coverage and others exclude personal information that, if disclosed, would prejudice or impair a person's reputation or security. In those states that keep social security numbers off the public record or that limit its disclosure, this exemption has a much more limited effect. Added to the debate is the Commonwealth's long-held policy that government officials should not question or limit the use to which citizens use public records. Given all of this, the Committee voted to exempt records that the law requires to be open.

At one point during the discussion, some people asked what made Virginia different enough that it was not discussing the model law adopted by other states. However, each state adopted slightly different provisions and exemptions and referred to laws different from those of the Commonwealth (*see* Appendix 7). Many of the provisions, as introduced to the Committee in the carryover bill, were identical to provisions adopted by other states. Of the six states that adopted or introduced such a statute, two applied the limitations to government agencies; the Commonwealth already applies many of these limitations to itself and does not need to include government agencies in its statute. Other states treated new and renewing subscribers of insurance plans differently; the Commonwealth did not. While all but the fifth limitation and the restrictions on continued use appeared in other states bills in virtually identical form, other provisions differed. The Committee's proposal adopted many of the provisions while incorporating Virginia law and policies into it and taking advantage of the test of time.

2. Use of Social Security Numbers - Public Records

During the 2004 Regular Session, the General Assembly passed HB 543 (Patron - May), a JCOTS recommendation, with a reenactment clause. The bill would have prohibited filing or creating public records that contain more than the last four digits of any unique identifying number, unless such use is required by law or the record is exempt from disclosure. The bill defined unique identifying number as any alphabetic or numeric sequence, or combination thereof, that is unique and assigned to a specific natural person at that person's request and includes, but is not limited to, social security number, bank account number, credit card number, military service number and driver's license number. The bill excludes from the definition any unique identifying number that an agency assigns to a natural person in place of a social security number for identification so long as it is used for a single, specific government purpose. Either preparers or filers of such documents would have to certify that the document complies with this prohibition before the documents could be filed. Because the enactment contains a reenactment clause, the 2005 Session of the General Assembly must reenact the provisions of the bill for it to become effective.

To address both privacy and identity theft concerns, the second proposal sought to keep information that could be used to access financial accounts, medical files and other similar personal identification information out of public circulation, unless the use was required by law. Beginning with documents created or filed after July 1, 2005, unless other laws require that an entire unique identifying number appear on a public record, this proposal would limit it to the last four digits. A "unique identifying number" is any alphabetic or numeric sequence, or combination thereof, that is (i) unique and (ii) assigned to a specific natural person (iii) at that person's request, and includes social security numbers, financial account numbers and drivers' license number.

Originally excluded from the definition were arbitrarily assigned numbers used for identification, in place of a social security number, for a single, specific government purpose (e.g., elections identification). This exemption enables government agencies to continue using alternative numbers that are not social security numbers. In addition, the Committee discussed two additional exemptions. The first would exclude payment information to the extent it is covered by a provision of the Government Data Collection and Dissemination Practices Act (§ 2.2-3808.1) that prohibits agencies and court clerks from disclosing certain account information. This exclusion would remove from the coverage of this proposal documents that only contain payment information, which already can not be disclosed to the general public. The second would exclude financial account numbers for non-revolving accounts, because disclosing this information would not allow anyone to increase the financial burden on the obligated party.

This proposal would limit unique identifying numbers on public records that have no privacy protections to no more than the last four digits. If the document is subject to a discretionary disclosure to the general public, it would have to be configured to prevent the disclosure of no more than the last four digits of such a number, similar to the requirement for marriage licenses as set out in § 32.1-267. It would also place the burden of checking the document on the filers and preparers by requiring some type of certification with flexibility for the agencies. As an alternative, agencies would be able to publish a list of documents that are protected from disclosure to the general public.

Like the first proposal, this one was the subject of much debate. Opponents argued that information companies gather much of their information from public documents and need that information to perform background checks, credit checks and other requested and required investigations. Credit bureaus and information companies use public records to assist law enforcement, companies and day care centers in performing legally required background checks to protect the public. Further, some opponents believe that credit bureaus would be unable to comply with federally mandated accuracy requirements without information from the public records, because they use the social security number to ensure that the information is connected to the right person.

Opponents also indicated that attempting to restrict the responsible use of social security numbers is not an effective way to address this problem. Law enforcement agencies and private companies use them to help combat identity theft and fraud. Other entities use them various purposes such as locating witnesses to crimes and helping make arrests, helping to locate pension beneficiaries, security/employment screening, helping to locate blood, bone marrow and organ donors, and preventing and investigating financial crime. They added that no studies have shown that public records are fueling identity theft and fraud.

Proponents argued that perpetrators have gathered the information used to commit identity theft from public records as diverse as military discharge papers and traffic tickets. Some convicted identity thieves have admitted on national television that they obtained information from, among other places, publicly available records. Further, in a recent study, the Government Accountability Office (GAO) found that the more social security numbers are used, the more likely they will be misused given the continued rise in identity crimes. The GAO cautioned that

policy makers would have to balance the protections that could occur from restrictions on their use with legitimate business needs for their use. This bill sets the balance at limiting their use on new public records where the information is not required and the document's disclosure is unlimited. Current public records are difficult to address until technology offers a solution.

State legislatures and courts have been working to remove unnecessary personally identifiable information from public records going forward and limit access to that information on previously filed documents or documents where the information is required. The private sector has already removed such information, like social security numbers, from deeds and other land records. This bill would have continued that policy and turned the focus to specific documents and specific uses. If the policy is to include these identifiers on all public records, then the law should state that requirement.

Given the controversy and the questions raised, the Committee opted not to recommend this proposal. Because of the reenactment clause, House Bill 543 (2004) will not become effective absent further legislative action by the 2005 General Assembly.

3. FOIA Exemption for Unique Identifying Numbers

Because the Committee supported the premise of protecting personal information as one means of decreasing the incidents of identity theft, they received and discussed an alternative to the second proposal. This alternative left public records and the information that they collect alone. Instead, it addressed the issue at the point of disclosure. The third proposal would enable public officials to exclude unique identifying numbers from disclosure under the Freedom of Information Act unless disclosure was otherwise required or allowed by law.

For the same reasons, the Committee opted not to recommend this proposal.

4. Social Security Numbers on Land Records

Along the same lines, the Committee discussed this holdover proposal from the Commission's 2003 study. It would require that any document submitted for recordation in the deed books of any Circuit Court clerk's office not contain a complete social security number after July 1, 2005. The proposal was based on a suggestion to the 2003 Advisory Committee on Consumer Protection that § 17.1-227 of the Code of Virginia be amended to add this requirement. Originally, it limited the appearance of social security numbers to the last four digits. The amended proposal would have kept the entire social security number off the documents recorded in the deed books.

The Commonwealth had already given the clerks of court the authority to refuse to accept any instrument submitted for recordation in the deed books that contained a social security number. During the 2004 Session of the General Assembly, the Commonwealth amended that provision

to place the responsibility for ensuring removal of the social security number on the attorney or party who prepared or submitted the instrument.

Seeing no need for further changes, the Committee opted not to recommend this proposal.

5. Personal Identification Information on Negotiable Instruments

The General Assembly passed HB 1424 (Patron - Dudley), which prohibits a person who accepts checks in the transaction of business from recording a date of birth upon the check as a condition of accepting the check. The section does not affect collection of a birth date for reasons unrelated to accepting the check, nor does it block a requirement that the payor provide his year of birth. This proposal is a natural extension of that bill and restricts the use of personal information that can be used to commit financial fraud and identity theft on all negotiable instruments. This measure limits the use of key information for access to financial records as a means of addressing both privacy and identity theft concerns.

The Committee questioned whether it would prohibit information necessary to complete the transaction or even to create a negotiable instrument. Not wanting to discuss it further, the Committee opted not to recommend this proposal.

6. Notice of Breach of Information Systems

This measure would require any state agency or business that owns or licenses a computerized database that includes personal information to disclose a breach of the security of that system to any resident of the Commonwealth whose unencrypted personal information may have been acquired by an unauthorized person. This proposal was not introduced during the 2004 Session, but was discussed with the approval of the legislator proposing it.

The Committee discussed this proposal based on a California law that required entities to provide notice to its citizens if specified personal information stored in a computer system had been compromised. Members of the Committee questioned how the law determines when a breach has occurred and when it requires companies and agencies to notify people. One concern raised was how companies would explain notifying its customers months, perhaps even years, after a breach when law enforcement officials told them to wait until after the completion of an investigation. Another member noted that California authorities are not happy with the results of their bill's implementation. Some members also believed that it was premature to discuss this proposal before it had formally been introduced in a legislative session.

The law in some areas has moved in the direction of notification when some compromise personal information. Furthermore, Courts are being to decide cases regarding liability over lack of, or inadequate, security precautions.

Because of questions about the practical effects of the proposal and concerns about whether it was premature, the Committee opted not to recommend this proposal.

7. Extending Sunset for Court Records Internet Postings Restrictions

After Mr. Dicks's presentation on the court clerks' view on efforts to limit confidential information on court records and noting that the provisions limiting them from posting certain information on court-controlled websites will expire on July 1, 2005, the Committee voted to recommend extending the prohibitions for two more years. The Committee expressed its hope that extending the provisions would give all parties more time to find a permanently workable solution.

8. Biometrics Study

As requested by Ms. Chappell in her presentation on the use of biometric technologies to verify identity at DMV, staff drafted a study resolution. The resolution also was based on the recommendation of the joint subcommittee established by House Joint Resolution 162 (2004). That joint subcommittee studied the desirability and feasibility of issuing driver's licenses and identification cards containing an embedded computer chip that stores biometric and other personal data. The Committee recommended amending the resolution to direct JCOTS to conduct the study.

IV. CONCLUSIONS

The Joint Commission on Technology and Science extends its sincere appreciation to everyone who participated in its work during the past year. We look forward to continuing to build on this work in 2005-2006.

Respectfully submitted,

Delegate Joe T. May, Chair
Senator Stephen D. Newman, Vice Chair
Delegate Kenneth C. Alexander
Delegate John A. Cosgrove
Senator Janet D. Howell
Delegate Sam A. Nixon, Jr.
Delegate Kenneth R. Plum
Delegate Harry R. Purkey
Delegate Thomas D. Rust
Senator Kenneth W. Stolle
Senator William C. Wampler, Jr.
Senator John Watkins

APPENDICES

Appendix 1

2004-2005 Commission Work Plan
(Adopted May 26, 2004)

Issues to Actively Study through Advisory Committees

COMPUTER CRIMES

ISSUE: Technology has brought new opportunities for old world criminals. Some of these individuals escape the law because statutes do not always address their activities, some because of problems with detection or underfunded law enforcement departments, and others because the individual's physical location is beyond the "arm of the law."

Since the Commonwealth enacted its first Computer Crimes Act in 1984, it has fought to keep pact with an ever-changing technology landscape. The legislature has amended it to include harassment, using encryption to further criminal activity, spam and forfeiture provisions. In the 2004 Regular Session, legislators introduced two proposals to extend criminal prosecutions to spreading computer viruses. This committee will examine recent events in computer activities and related legislative proposals to maintain the effectiveness of the Computer Crimes Act.

CHARGE: To study Virginia's Computer Crimes Act and related laws in light of current activities and technologies; recommend any necessary amendments to criminalize certain computer-related conduct, such as spreading a computer virus or other malicious code; and evaluate the need for special laws on computer-related conduct.

TOPICS: Computer Viruses as Trespass (HB 566 / SB 275) – Introduced in the 2004 Session and continued by the House Committee on Science and Technology, these bills would have created a separate criminal charge for knowingly and maliciously inserting a computer virus into a computer, computer program, computer software, or computer network of another without the knowledge and permission of the owner.

Virginia Computer Crimes Act review.

INTEGRATED GOVERNMENT (I-GOV): THE FUTURE OF GOVERNMENT IN THE ELECTRONIC AGE

ISSUE: The Commonwealth is recognized nationally and internationally as a leader in the development of what has become known as electronic government. However, the Commonwealth has also evolved beyond merely digitizing the services and materials it has always offered to re-thinking its underlying policies and processes. This re-thinking ("Integrated Government" or "I-GOV") involves integrating paper- and jurisdiction-based governmental processes. At its core, it contemplates a transformation from the way government operated prior to the information age.

CHARGE: To explore the issues created or enhanced by the transformation of government in the electronic age.

TOPICS: Continue work with VITA on its implementation and operation.

Continue discussions on information technology and procurement reform.

Assess the implications of outsourcing on the Virginia economy and government. As more companies and governments grapple with the implications of outsourcing functions and jobs to foreign countries, legislatures around the country have attempted to use the law to address its impact. What does this mean for Virginia?

Radio frequency identification (RFID) first appeared in tracking and access applications during the 1980s. These wireless AIDC systems allow for non-contact reading and are effective in manufacturing and other hostile environments where bar code labels could not survive. RFID has established itself in a wide range of markets including livestock identification and automated vehicle identification (AVI) systems because of its ability to track moving objects. The U.S. Department of Defense will give radio frequency identification technology a massive boost with a new policy requiring its suppliers to use RFID chips. The Defense Department's policy requires that by January 2005 all suppliers embed passive RFID chips in each individual product if possible, or otherwise at the level of cases or pallets. The policy applies to everything except bulk commodities such as sand, gravel or liquids. The department said the policy would allow it to streamline its supply-chain and business processes. Wal-Mart and other retailers also are planning to require RFID chips from their suppliers in the near future. As RFID use hits the main stream, Virginia will have to determine whether and how it will utilize RFID in its procurement processes and otherwise.

Electronic communication meetings: the exemptions set out in the *Code of Virginia* expire on July 1, 2005. This committee will review public bodies' use of electronic communications for holding meetings and recommend the future of this option.

Address the issues raised by the evolution of government documents to the electronic form (e.g., archiving and retention) and the mandate for electronic filing (e.g., Uniform Real Property Recordation Act).

PRIVACY: Information and Technology

ISSUE: Computers allow businesses and government to gather, aggregate and use information in ways never before imagined. The impact on individuals of each stage of the process must be evaluated to prevent misuse and establish a proper balance between the individual and the business or government. For example, online transactions typically require an individual to reveal personal information, much of which appears to be unnecessary to the transaction. While an individual can simply refuse to provide the information in the offline world, this action may prevent completing the transaction in the online world.

In the government sphere, the development of new technologies has challenged the balance between civil liberties and security that has been a long-established principle embedded in the constitutions of the United States and the Commonwealth of Virginia. As governments are being asked to fund, authorize, limit or prohibit the use of many of these technologies to address the needs of law enforcement and security agencies, these needs must be balanced against those civil liberties. Technologies available today can track a person's movement, listen to his conversations, assess the speed of his vehicle, and look inside his house all from a remote location and without his knowledge. As these technologies become more invasive and their use more clandestine, the potential for unchecked abuse threatens to impinge civil liberties.

CHARGE: Review current privacy laws and practices as they pertain to information and its treatment both in cyberspace and physical space, including the impact of criminal laws and document filing requirements.

Propose policies and guidelines for public bodies to evaluate the use of potentially invasive technologies when determining whether to support their use financially or to authorize or prohibit their use.

TOPICS: Use of Social Security Numbers (HB 753); Use of Unique Identifying Numbers on Public Records (HB 543) – The Commission recommended these bills for the 2004 Session. The House Committee on Science and Technology carried over HB 753 to 2005 Session; the General Assembly passed HB 543 with a reenactment clause.

Examine the results of the Virginia Supreme Court's study on personal information on records filed with the court and on court records. This study includes the state and federal legal requirements and common practices.

Model Policy for Access to Court Records – prepared on behalf of the Conference of Chief Justices and the Conference of State Court Administrators by the National Center for State Courts and the Justice Management Institute, this model policy was drafted to provide guidance to state and local courts on public access to personal information in court records and to provide consistency of access to court records.

Workplace privacy - During the 2003 Session, the Commission proposed legislation (HB 1887 / SB 1289) to address covert electronic monitoring in the workplace. Continue discussing the concerns regarding this legislation and working with the organizations that raised those concerns.

Review the various types of potentially invasive technologies available for use, determine the current legal requirements of their use, the reasons for their use, their impact on civil liberties, and any safeguards that are or should be used to mitigate negative impacts. These technologies include radio frequency identification, tracking systems, facial recognition systems, hidden cameras, spyware, photo monitoring systems and Internet wiretaps.

Impact of modern technologies on civil liberties (HB 1304) and use of event data recorders (HB 697) – The House Committee on Science and Technology continued these bills in the 2004 Session and referred them to JCOTS for study.

NANOTECHNOLOGY

ISSUE: In December of 2003, the federal government enacted the 21st Century Nanotechnology Research and Development Act (S189) authorizing almost $3.7 billion in government funding for nanotechnology research and development (R&D). The legislation emphasizes the establishment of R&D Centers in academia and government. There are now over 50 institutes and centers dedicated to nanotechnology research. For example, the National Science Foundation has established the National Nanotechnology Infrastructure Network - comprised of 13 university sites that will form an integrated, nationwide system of user facilities to support research and education in nanoscale science, engineering and technology. Similarly, there are currently 15 government agencies with R&D budgets dedicated to nanotechnology.

The Commonwealth has a tradition of industrial excellence, from large enterprises to entrepreneurs, which has existed in traditional industries, as well as in emerging industries. Now, it has the opportunity to build on its existing expertise and become a national and international leader in nanomanufacturing, an emerging industry. Nanotechnology promises to transform most industries and will have a particularly profound impact on health care, homeland security, national defense and the national infrastructure. Nanotechnology is poised to become the largest government science initiative since the space race as demonstrated by the president's FY04 budget request of $849 million for

nanotechnology research and development (R&D). According to one report, more than $3 billion will have been invested worldwide in nanotechnology R&D in 2003 increasing to a predicted $1 trillion by 2015. California, Colorado, Georgia, Illinois, New York and Texas have already announced and demonstrated their commitment to nanotechnology. While manufacturing remains central to the country's economic growth and improving standard of living, nanomanufacturing will require new skills and new equipment. The Commonwealth has an existing national recognition in nanotechnology, as its leading research universities and national laboratories continue to produce groundbreaking work in biomedicine, electronically functional nanomaterials, alternative energy resources, and nanostructured coatings. Additionally, the Commonwealth has existing industrial strengths where nanotechnology will play a critical role, including health care, aerospace, semiconductors, communications, information technology, chemicals, and power generation.

CHARGE: To identify nanotechnology research and economic development opportunities for the Commonwealth and consider the efficacy of creating a statewide, comprehensive and coordinated strategy to secure additional federal research and development funds and to boost commercial activity in this fast-emerging sector.

TOPICS: HJ 120, adopted by the 2004 General Assembly, directs JCOTS to identify nanotechnology research and economic development opportunities for the Commonwealth and consider the efficacy of creating a statewide, comprehensive and coordinated strategy to secure additional federal research and development funds and to boost commercial activity.

Explore industry efforts regarding nanotechnology across the Commonwealth. These efforts include NVTC's current investigation of the potential for a Nanotechnology Accelerated Development Center in Northern Virginia to provide rapid prototyping demonstrations of nanotechnology-enabled breakthrough capabilities for government programs and industrial products, to situate the facility for convenient physical access by government agencies and for robust virtual access by government, industry and academia; to accelerate the commercialization of nanotechnology through proof-of-concept, rapid design, and prototyping projects; to build and retain a world-leading nanotechnology workforce by establishing an attractive domestic business community for college and university graduates which benefits all of Virginia; to capture dominant market share for U.S. nanotechnology manufacturers through early market entry; to leverage the large investment in research, training and infrastructure by the National Nanotechnology Initiative (NNI); and to initiate educational outreach for K-12 grade students in nanoscience and nanotechnology, as well as career opportunities in nanotechnology throughout Virginia.

Issues to Actively Study through Commission Meetings

SECURING DATABASES AND PERSONAL COMPUTERS

Online criminals are attacking corporate and government networks more frequently, costing businesses an estimated $666 million in 2003, according to a survey of computer security executives conducted by CSO [Chief Security Officer] magazine in cooperation with the U.S. Secret Service and the CERT cybersecurity center at Carnegie Mellon University in Pittsburgh. Both internal threats, such as those from disgruntled or recently fired employees, and external threats, such as those from hackers, are rising every year. These networks are essential to the daily operations of businesses and government agencies.

While firewalls, virus protection software, encryption and other technologies can help protect systems, they do not and can not offer complete protection. Defective and readily exploitable software code, lax security measures, and reliance on a myriad of passwords remain the predominate cause of many security breaches. Furthermore, as businesses and government move sensitive information onto portable computers and conduct business in numerous locations, security has become a key factor. Losing a single computer could compromise business plans, systems and even individuals. Making matters more critical is the move to recycle old computers, instead of destroying them. A proper plan for rendering all critical information unreadable and irretrievable is vital in today's society. The Commission will hear testimony and witness demonstrations of how easily deleted information can be retrieved.

ADMINISTRATION UPDATE

The Code requires the Secretary of Technology, the Chief Information Officer and the President of the Center for Innovative Technology to work with and/or report to the Commission on their initiatives and plans. These three individuals will brief the Commission on their work and plans.

Studies to Monitor

- HJ 631 (2003) – Final year of the joint subcommittee studying the protection of court records to review the findings and recommendations of the Executive Secretary of the Supreme Court concerning information in court records and recommend necessary changes in the statutory law.
- HJ 6 (2004) - Creates a joint subcommittee to study the Virginia Public Records Act, electronic records, and their effect on the state depository system.
- HJ 162 (2004) - Establishes a joint subcommittee to study the desirability and feasibility of issuing driver's licenses and identification cards containing an embedded computer chip that stores biometric and other personal data.
- HJ 176 (2004) - Creates a joint subcommittee to study the impact of collecting remote sales taxes on the economy of the Commonwealth, including the impact on revenue and small businesses.

Appendix 2

2004 - 2005 JCOTS Calendar

2004

All meetings will be in House Room D.

- **May 26 –** 2004 Organizational Meeting (9:30 a.m.)
- **June 30 –** Integrated Government Advisory Committee (1st Meeting) (10:00 a.m.)
- **July 7 –** Privacy Advisory Committee (1st Meeting) (9:30 a.m.)
- **August 3 -** Tour of Blacksburg and Virginia Tech
- **August 4** – Nanotechnology Advisory Committee (1st Meeting) (1:30 p.m.)
- **August 10 –** Computer Crimes Advisory Committee (1st Meeting) (9:30 a.m.)
- **August 17 -** Integrated Government Advisory Committee (2nd Meeting) (9:30 a.m.)
- **August 18 -** Privacy Advisory Committee (2nd Meeting) (1:30 p.m.)
- **September 8 -** Commission Meeting on *Computer Security* (9:30 a.m.)
- **September 21 -** Computer Crimes Advisory Committee (2nd Meeting) (1:00 p.m.)
- **September 22** - Nanotechnology Advisory Committee (2nd Meeting) (1:30 p.m.)
- **October 5** - Integrated Government Advisory Committee (3rd Meeting) (9:30 a.m.)
- **October 6 -** Privacy Advisory Committee (3rd Meeting) (1:30 p.m.)
- **October 19 -** Computer Crimes Advisory Committee (3rd Meeting) (9:30 a.m.)
- **October 20 -** Nanotechnology Advisory Committee (3rd Meeting) (1:30 p.m.)
- **November 16 -** Integrated Government Advisory Committee (4th Meeting) (1:30 p.m.)
- **November 17 -** Privacy Advisory Committee (4th Meeting) (1:30 p.m.)
- **December 1 -** Commission Meeting (9:30 a.m. - GAB) (*Topic: 2005 Legislative Proposals*)

Appendix 3

JCOTS 2004 Advisory Committees[1]
(Final 12/31/2004)

Joint Advisory Committee on Computer Crimes (17)
Delegate May (JCOTS), Delegate Albo (VSCC)

NAME	ADDRESS	PHONE & FAX	E-MAIL
Michael Aisenberg	VeriSign, Inc. 21345 Ridgetop Circle Dulles, VA 20166	P - 202-973-6600 F - 202-466-9103	maisenberg@verisign.com
W. Scott Arnott	Chief Technology Officer Zel Technologies, LLC 54 Old Hampton Lane Hampton, VA 23669	P – 757-722-5565	scott.arnott@zeltech.com
William B. Baker	Wiley Rein & Fielding LLP 1776 K Street, NW Washington, DC 20006	P - 202-719-7255 F - 202-719-7049	wbaker@wrf.com
Steven D. Benjamin	11 South 12th Street, Suite 302 Richmond, Virginia 23219	P - 804-788-4444 F - 804-644-4512	sdbenjamin@aol.com
Charles D. Curran	America Online, Inc. 22000 AOL Way Dulles, VA 20166-9323	P - 703-265-3153 F - 703-265-1239	cdcurran@aol.com
Steve DelBianco	Association for Competitive Technology 9123 Horner Court Fairfax, VA 22031	P - 703-615-6206 F - 703-783-0322	sdelbianco@actonline.org
Cynthia H. de Lorenzi	PatriotNet, Inc. 4031 University Drive, 2nd Floor Fairfax, VA 22030	P - 703-797-1888 Ext. 211 F - 703-273-9236	cdelorenzi@patriot.net
Brian Dunphy	Dir. of Global Analysis Operations Managed Security Services Symantec Corporation 2800 Eisenhower Avenue Alexandria, VA 22314	P - 703-373-5150	brian_dunphy@symantec.com
Magnolia Mansourkia	MCI Network Services, Inc 1133 19th Street, NW Washington, DC 20036	P - 202-736-6448 F - 202-736-6460	maggie.mansourkia@mci.com
Thomas W. Mastaglio	MYMIC LLC 200 High Street, Suite 308 Portsmouth, VA 23704	P - 757-391-9200 F - 757-391-9098	tom.mastaglio@mymic.net
Russell E. McGuire	Office of the Attorney General 900 East Main Street Richmond, VA 23219	P – 804-786-0086 F – 804-786-1991	rmcguire@oag.state.va.us

[1] Numbers in parentheses represent the number of non-Commission members on each committee.

NAME	ADDRESS	PHONE & FAX	E-MAIL
Gregory C. Mullen	Deputy Chief Virginia Beach Police Department 2509 Princess Anne Road Municipal Center Bldg. 11 Virginia Beach, VA 23456	P – 757-427-4141 F – 757-427-9163	gmullen@vbgov.com
Brian H. Murray	Cyveillance, Inc. 1555 Wilson Boulevard, Suite 404 Arlington, VA 22209-2405	P - 703-312-1252 F - 703-312-0536	bmurray@cyveillance.com
Jeffrey H. Nelson	Nixon & Vanderhye P.C. 1100 N. Glebe Road Arlington, VA 22201	P - 703-816-4023 F - 703-816-4100	jhn@nixonvan.com
Jim Plowman	Commonwealth's Attorney Loudoun County 20 E. Market Street Leesburg, VA 20176	P - 703-777-0242	oca@loudoun.gov
Greg Redfern	Computer Sciences Corporation 3160 Fairview Park Dr. M/C 263 Falls Church, VA 22042	P - 703-876-1452 F - 703-205-0133	gredfern@csc.com
William Wiita	Bedford County Sheriff's Office 1345 Falling Creek Road Bedford, VA 24523	P - 434-534-0661 F - 434-534-0663	rwiita@bedfordsheriff.org

Integrated Government (18)
Delegate Nixon, Delegate Plum, Senator Howell

NAME	ADDRESS	PHONE & FAX	E-MAIL
Jennifer Angelino	Nextel Communications 2001 Edmund Halley Drive Reston, VA 20191	P - 703-906-5424 F - 703-433-4142	jennifer.angelino@nextel.com
Skip Cohen	AVAYA 4250 N. Fairfax Drive, 10th Floor Arlington, VA 22203	P - 410-859-2949 F - 410-859-2949	sdcohen@avaya.com
Richard E. Fore	City of Charlottesville P. O. Box 911 Charlottesville, VA 22902	P - 434-970-3199 F - 434-970-3880	rickfore@charlottesville.org
Anne Gavin	Microsoft Corporation 1244 Woodbrook Court Reston, VA 20194	P - 703-904-8146 F - 703-904-8219	annega@microsoft.com
Scott Hommer	Venable LLP 8010 Towers Crescent Dr., Ste 300 Vienna, Virginia 22182-2707	P – 703-760-1600 F – 703-821-8949	jshommer@venable.com
Barry Ingram	EDS 13600 EDS Drive Herndon, VA 22124	P - 703-742-2575 F - 703-742-2701	barry.ingram@eds.com
Thomas D. Lash	Science Applications International Corp. (SAIC) 9390 Worthington Drive Bristow, VA 20136	P - 703-753-1146 F - 703-802-9440	lasht@saic.com

NAME	ADDRESS	PHONE & FAX	E-MAIL
Bennett I. (Ben) Lewis	CGI-AMS 600 East Main Street Richmond, VA 23219	P - 804-648-3906 F - 804-648-4317	ben.lewis@cgi-ams.com
David J. Molchany	Fairfax County Government 12000 Government Center Pkwy Fairfax, VA 22035	P - 703-324-4775 F - 703-324-3956	dmolch@fairfaxcounty.gov
Michael W. Newton	Newton & Associates, LLC 2851 Ambergate Terrace Midlothian, VA 23113-2176	P - 804-794-8144	mike@improvingresults.com
Fred Norman	Commonwealth of Virginia Consulting (CVC) P. O. Box 74355 Richmond, VA 23236	P - 804-690-1497 F - 804-639-3730	fred.norman@cvconline.net
Daniel G. Oakey	Advantus Strategies, L.L.C. 1011 East Main Street, 4th Floor Richmond, VA 23219	P - 804-228-4505 F - 804-228-4501	boakey@advantusstrategies.com
Gregory W. Phillips	Advanced Technology Systems 901 East Byrd Street, Suite 1340 Richmond, VA 23219	P - 804-775-8520 F - 804-775-8559	gphillips@atsva.com
Shawn Rodriguez	Nortel Networks 951 E. Byrd Street, Suite 510 Richmond, VA 23219	P - 804-225-7008 F - 804-225-7050	shrodrig@nortelnetworks.com
James J. Villers	3133 Inlet Road Virginia Beach, VA 23454	P - 757-481-6398	betty@whro.net
Rodney T. Willett	1 Raven Rock Lane Richmond, VA 23229	P - 804-741-3231 C - 804-363-1534	rodwillett@comcast.net
Bruce E. Wine	Dell, Inc. 3621 Rivermist Court Midlothian, VA 23113	P - 804-897-5372 F - 804-897-5373	bruce_wine@dell.com
Mary Zdanius	Gateway Professional 4711 Archduke Court Glen Allen, VA 23060	P - 804-301-8124 F - 804-747-5026	mary.zdanius@gateway.com

Nanotechnology (25)
Delegate Purkey, Senator Wampler, Delegate Cosgrove

NAME	ADDRESS	PHONE & FAX	E-MAIL
Frank Cavaliere	Office of Senator George Allen Senator Russell Office Building, Room 204 Washington, DC 20510	P - 202-224-4024 F - 202-228-3561	frank_cavaliere@allen.senate.gov
Richard O. Claus	Virginia Polytechnic Institute & State University Fiber&Electro-Optics Research Ctr 106 Plantation Road Blacksburg, VA 24060	P - 540-231-7203 F - 540-231-4561	roclaus@vt.edu
Steve Danziger	BAE Systems 9300 Wellington Road Manassas, VA 20110	P - 703-367-3478 F - 703-367-5234	steven.danziger@baesystems.com

NAME	ADDRESS	PHONE & FAX	E-MAIL
H. Frederick Dylla	Jefferson Lab 12000 Jefferson Avenue MS 7A Newport News, VA 23606	P - 757-269-7450 F - 757-269-6357	dylla@jlab.org
Charles Gause	Luna Innovations Incorporated 2851 Commerce Street Blacksburg, VA 24060	P - 540-953-4297 F - 540-951-0760	gausec@lunainnovations.com
Daniel J. Gonzalez	Scheer Partners, Inc. 7901 Jones Branch Drive, #130 McLean, VA 22102	P - 703-288-2700 F - 703-288-0975	dgonzalez@scheerpartners.com
Richard V. Gregory	Old Dominion University 1260 Barn Brook Road Virginia Beach, VA 23454	P - 757-683-3277	rgregory@odu.edu
B. Frank Gupton	Executive Director Boehringer Ingelheim 2820 North Normandy Drive Petersburg, VA 23805-9372	P - 804-504-8803	
Robert Hull	University of Virginia Department of Materials Science 116 Engineers Way Charlottesville, VA 22904	P - 434-982-5658 F - 434-982-5660	hull@virginia.edu
Dimitris E. Ioannou	George Mason University Electrical and Computer Engineering Department Fairfax, VA 22030	P - 703-993-1580 F - 703-993-1601	dioannou@gmu.edu
Jim Kadtke	Office of Senator John Warner 225 Russell Senate Office Building Washington, DC 20510	P - 202-224-6958 F - 202-224-6079	james_kadtke@warner.senate.gov
Philip D. Lane	McGuireWoods, LLP 1750 Tysons Boulevard, Ste. 1800 McLean, VA 22102-4215	P - 703-712-5069 F - 703-712-5296	plane@mcguirewoods.com
Dennis M. Manos	College of William and Mary The Brafferton Kitchen P. O. Box 8795 Williamsburg, VA 23185	P - 757-871-9581 F - 757-221-3540	dmanos@as.wm.edu
Robert J. Mattauch	VCU School of Engineering 601 West Main Street Richmond, VA 23284-3068	P - 804-828-0190 F - 804-828-9866	rjmattau@vcu.edu
Scott E. McNeil	Science Applications International Corp. (SAIC) 1710 SAIC Dr. (MS 2-3-1) McLean, VA 22102	P - 703-676-5170 F - 703-676-2298	scott.e.mcneil@saic.com
John Noftsinger	Associate Vice President of Academic Affairs for Research and Public Service James Madison University ISAT/CS Building 365, MSC 4107 Harrisonburg, VA 22807	P - 540-568-2700 F - 540-568-1784	noftsijb@jmu.edu
Alfonso Victor Peña	nanoTITAN, Incorporated 10705 Burr Oak Way Burke, VA 22015-2405	P - 703-250-2549 F - 703-250-1905	avpena@nanotitan.com
Mark J. Shuart (liaison)	NASA Langley Research Center Mail Stop 121 Hampton, VA 23681	P - 757-864-3492 F - 757-864-7792	mark.j.shuart@nasa.gov

NAME	ADDRESS	PHONE & FAX	E-MAIL
Robert E. Smartschan	Hampton Roads Tech. Council Kaufman & Canoles, P.C. 150 West Main Street P. O. Box 3037 Norfolk, VA 23514-3037	P - 757-624-3221 F - 757-624-3169	resmartschan@kaufcan.com
Richard H. Smith, II	Nanoverse, LLC 2121 Jamieson Ave., #505E Alexandria, VA 22314	P - 703-567-0404 F - 703-567-0405	rhsmith@nanoverse.net
Sharon Smith	Lockheed Martin Corporation 6801 Rockledge Drive Bethesda, MD 20817	P - 301-897-6267 F - 301-897-6654	sharon.smith@lmco.com
T. S. Sudarshan	Materials Modification Inc. 2721-D Merrilee Drive Fairfax, VA 22031	P - 703-560-1371 Ext. 11 F - 703-560-1372	sudarshan@matmod.com
Bruce J. Swenson	Science Applications International Corp. (SAIC) 1710 SAIC Drive (MS 9-1-2) McLean, VA 22102	P - 703-676-5117 F - 703-821-1037	swensonbr@saic.com
Usha Varshney	National Science Foundation 4201 Wilson Boulevard Arlington, VA 22230	P - 703-292-8339 F - 703-292-9124	uvarshne@nsf.gov
Charles F. Wieland	Burns Doane Swecker & Mathis The Atlantic Nano Forum 1737 King Street, Suite 500 Alexandria, VA 22314	P - 703-836-6620 F - 703-836-2021	chadw@burnsdoane.com

Privacy (12)
Delegate May, Senator Watkins, Delegate Alexander

NAME	ADDRESS	PHONE & FAX	E-MAIL
Elizabeth Barry-Kessler	AOL 11200 Chestnut Grove Sq. #304 Reston, VA 20190	P - 703-481-9181 F - 703-265-4786	elizkessler@aol.com
Jean Cantrell	EDS 1331 Pennsylvania Avenue, NW # 1300 N Washington, DC 20004	P - 202-637-4965 F - 202-637-6757	jean.cantrell@eds.com
Eric J. Ellman	CDIA 1090 Vermont Avenue, NW Suite 200 Washington, DC 20005-4905	P - 202-408-7407 F - 202-371-0134	eellman@cdiaonline.org
Dennis M. Frye	Roanoke City Public Schools 40 Douglass Avenue, N.W. Roanoke, VA 24012	P - 540-853-1147 F - 540-510-4310	dfrye@roanoke.k12.va.us
Vance C. Gudmundsen	Capital One Financial Corporation 1680 Capital One Drive McLean, VA 22102	P - 703-720-2292 F - 703-720-2227	vance.gudmundsen@capitalone.com

NAME	ADDRESS	PHONE & FAX	E-MAIL
Thomas W. J. C. McCrystal	creative perspectives, inc. 103 E. Water Street, Suite 201 Charlottesville, VA 22902	P - 434-971-6795 F - 434-971-8662	tmc@creative-perspectives.com
Daniel Nestel	LexisNexis/Reed Elsevier 1150 18th Street, NW, Suite 600 Washington, DC 20036	P – 202-857-4643 F – 202-857-8294	daniel.nestel@lexisnexis.com
Alok C. Nigam	Global InfoTek, Inc. 1920 Association Drive, Suite 200 Reston, VA 20191	P - 703-652-1600 Ext. 239 F - 703-832-0529	nigam@globalinfotek.com
Gregory Robinette	Robinette Industries and Consulting 6141 Sedgefield Drive Norfolk, VA 23513	P - 757-858-5986 F - 757-858-5986	gregrobinette@cox.net
Guillermo A. Söhnlein	Aptela 1616 Anderson Road McLean, VA 22102	P - 703-386-1500 Ext. 9207 F - 703-386-1500	guillermo@aptela.com
Gerard M. Stegmaier	Wilson Sonsini Goodrich & Rosati 11921 Freedom Drive, Suite 600 Reston, VA 20190-5634	P - 703-734-3109 F - 703-734-3199	gstegmaier@wsgr.com
Brian Tretick	Ernst & Young LLP 8484 Westpark Drive McLean, VA 22102	P - 703-747-0901 F - 703-747-0175	brian.tretick@ey.com

Appendix 4

JCOTS Recommended Legislative Proposal Summaries (as introduced)

COMPUTER CRIMES LEGISLATION

HB 2471
Virginia Computer Crimes Act; penalties. Updates the Virginia Computer Crimes Act to include recommendations made by the 2004 joint study on Computer Crimes by the Joint Commission on Technology and Science and Virginia State Crime Commission. The bill also amends the Computer Trespass statute to require that actions be taken with malicious intent before they are considered criminal and adds unauthorized installation of software on the computer of another, disruption of another computer's ability to share or transfer information, and maliciously obtaining computer information without authority as additional crimes of computer trespass, a Class 1 misdemeanor. Lastly, the bill reduces the threshold for a felony to $1,000.

HB 2472
Computer crimes; penalties. Updates the Virginia Computer Crimes Act to include recommendations made by the 2004 Joint Commission on Technology and Science and Virginia State Crime Commission joint study on Computer Crimes. The bill redefines computer invasion of privacy involving the unauthorized gathering of identifying information and punishes subsequent offenses, transferring the information to another or use of the information as a Class 6 felony. Currently, the offense is punishable only as a Class 1 misdemeanor. Additionally, the bill adds the fraudulent gathering of such information as a new crime and punishes it as a Class 6 felony and increases the crime to a Class 5 felony if a person transfers the information to another or uses the information.

HB 2473
Virginia Computer Crimes Act; hacking; penalties. Updates the Virginia Computer Crimes Act to include recommendations made by the 2004 joint study on Computer Crimes by the Joint Commission on Technology and Science and Virginia State Crime Commission. The bill streamlines language and criminalizes circumventing computer security measures, commonly known as hacking. The bill also consolidates criminal procedure provisions into Title 19.2.

PRIVACY LEGISLATION

HB 2052
Clerks of court; posting certain information on the Internet; prohibitions. Extends the sunset clause prohibiting clerks from posting certain information on a court-controlled website from July 1, 2005, to July 1, 2007.

HB 2468
Event data recorders; vehicle manufacturers; disclosure. Requires a manufacturer of a new motor vehicle sold or leased in the Commonwealth that is equipped with one or more recording devices, commonly referred to as "event data recorders" (EDR) or "sensing and diagnostic modules" (SDM), to disclose that fact in the owner's manual for the vehicle. The bill also requires a seller or lessor of a new vehicle to conspicuously disclose the fact prior to sale or lease. The bill applies to all motor vehicles manufactured for model year 2007 and later.

HB 2482
Personal Information Privacy Act; restricting the use of social security numbers. Amends the Personal Information Privacy Act to prohibit (i) intentionally communicating an individual's social security number to the general public; (ii) printing an individual's social security number on any card required for the individual to access or receive products or services; (iii) requiring an individual to use his social security number to access an Internet website, unless an authentication device is also required; or (iv) mailing a package with the social security number visible from the outside. The bill exempts public bodies and public records.

The bill also amends the Virginia Consumer Protection Act to prohibit a supplier from using a consumer's social security number when the consumer requests that his driver's license number be used. Current law requires that a supplier only provide an alternate number if the consumer so requests in writing. This bill provides consumers with an option other than providing their social security numbers and writing to the supplier for a new number.

INTEGRATED-GOVERNMENT LEGISLATION

HB 2051
Virginia Public Procurement Act; methods of procurement. Requires approval of the Chief Information Officer of the Commonwealth for the purchase of information technology and telecommunications goods and services from a public auction or off of another public body's contract.

HB 2054
Alternative Dispute Resolution; pilot project. Allows the Virginia Information Technologies Agency (VITA) to promulgate administrative rules concerning the use of alternative dispute resolution in lieu of the provisions set forth in the Virginia Public Procurement Act concerning procurement protests. The Chief Information Officer of the Commonwealth must report to the General Assembly on the implementation of the rules. The pilot project will expire on July 1, 2008.

HB 2672
Virginia Freedom of Information Act; meetings exemption. Amends an existing meetings exemption to allow for closed meetings to discuss records exempt from public disclosure relating to the Public-Private Education Facilities and Infrastructure Act (PPEA).

SB 1196

Freedom of Information Act; electronic communication meetings. Reduces the notice required for electronic communication meetings from 30 days to seven working days. The bill also (i) eliminates the 25 percent limitation on the number of electronic meetings held annually; (ii) eliminates the requirement that an audio or audio/visual recording be made of the electronic communication meeting, but retains the requirement that minutes be taken pursuant to § 2.2-3707; (iii) allows for the conduct of closed meetings during electronic meetings; (iv) changes the annual reporting requirement from the Virginia Information Technology Agency to the Virginia Freedom of Information Advisory Council and the Joint Commission on Technology and Science; and (v) expands the type of information required to be reported. The bill specifies that regular, special, or reconvened sessions of the General Assembly held pursuant Article IV, Section 6 of the Constitution of Virginia are not meetings for purposes of the electronic communication meeting provisions. The also bill defines "electronic communication means." The bill is a recommendation of the Joint Commission on Technology and Science.

JCOTS LEGISLATION

HB 2586

Joint Commission on Technology and Science; clarifications for collegial bodies. Conforms the Joint Commission on Technology and Science's requirements to meet legislative guidelines adopted by the Joint Rules Committee. The bill also makes procedural amendments such as reducing the quorum from six to five members, increasing the term of the chair and vice-chair to a two-year term coincident with the term of office for House members, and changing references from Commission to JCOTS.

Appendix 5

Outline of the Electronic Meetings Proposal of the Integrated Government Advisory Committee (as compared to the FOIA Council recommendation)

	2.2-3708	Acts of Assembly	Proposed
Entities subject to the provisions	Any state public body	State public bodies (i) in the legislative branch or (ii) with members who reside or work more than 55 miles from the meeting location	Any state public body
Types of meetings allowed	Telephonic or audio/visual communication	Audio/visual communications only	Telephonic or audio/visual communication
Notice	30 days	7 Days	7 working days
Meeting Locations Public Access **I-Gov/FOIA Council Difference*	A quorum must be physically assembled in one location;	Three members, or a quorum of the public body if less than three must be at locations that are (i) in Virginia and (ii) open to the public.	*I-Gov:* A quorum of the public body must be at locations that are (i) in Virginia and (ii) open to the public. *FOIA Subcommittee:* Quorum in one physical location: After the quorum is established, other members may join the meeting from locations that are not in Virginia or are not open to the public.
Public Access to Locations **I-Gov/FOIA Council Difference*	After a quorum is established, other members of the public body may meet from remote locations that are (i) in Virginia and (ii) open to the public	After the presence of three members or a quorum is established, other members may join the meeting from locations that are not in Virginia or are not open to the public.	*I-Gov:* After a quorum is established, other members may join the meeting from locations that are not in Virginia or are not open to the public. *FOIA Subcommittee:* All remote sites must be open to the public.

	2.2-3708	Acts of Assembly	Proposed
Reporting	Report must be filed with VITA by July 1 of each year identifying the total number of meetings held by the public body, the dates of the meetings, and the number and purpose of those meetings conducted electronically.	Report must be filed with JCOTS and the FOIA Council by Sept. 15 of each year identifying the total number of electronic meetings, the dates and purposes of the meetings, and for each electronic meeting indicate the number of sites, the type of electronic communications used, the number of participants, the number of remote participants, a summary of public comment about electronic meetings, and a summary of the public body's experiences with electronic meetings.	Report must be filed with JCOTS and the FOIA Council by Dec.15 of each year identifying the total number of electronic meetings, dates and purposes of the meetings, and the number of sites for each electronic meeting, the type of electronic communications used, the number of participants, the number of remote participants including the identity of members at the remote sites, a summary of public comment about electronic meetings, and a summary of the public body's experiences with electronic meetings.
Recording	Public body must make an audio recording of telephonic meetings and an audio/visual recording of audio/visual meetings. The recording must be preserved for three years.	Public body must make an audio or audio/visual recording of the meeting. The recording must be preserved for three years.	No audio or audio/visual recording required. Meetings subject to regular minute requirements at § 2.2-3707. § 2.2-3707 is amended to require that minutes of electronic meetings include the identity of members participating remotely, the identity of members physically assembled at the central meeting location, and the identity of members who monitored the meeting electronically.
Closed Meetings	Prohibited	Allowed	Allowed
Limit on annual Number of electronic meetings	A public body may not hold more than 25% of its meetings annually by electronic communications means, except in the case of an emergency.	No limitation on number of electronic communications meetings.	No limitation on number of electronic communications meetings. At least one meeting annually must be held where all members of the public body are physically assembled.

Appendix 6
Virginia Beach General Order 93.06 - 02/19/02
Facial Recognition Utilization/Procedures

Purpose:

The Virginia Beach Police Department is committed to the safety and security of the citizens and visitors of Virginia Beach. To ensure this commitment, the Virginia Beach Police Department constantly strives to research and utilize the latest technology to enhance the performance of departmental members. To that end, the Department is enhancing its current video technology capabilities with the introduction of Biometrics in the form of facial recognition technology.

Definition:

1. Biometrics - Automated methods of recognizing and identifying a person based on physiological or behavioral characteristics such as fingerprinting, voice patterns, or facial recognition.

2. Facial Recognition Technology - The automated process of converting an image or photo into a mathematical, computer algorithm as a basis for recognition and potential identification. The software creates a digital map of an individual's face by translating the contours into mathematical formulas that are nearly as distinguishable as fingerprints.

Procedures:

1. Database:

A photographic database of wanted criminals with outstanding felony warrants, or certain misdemeanors that involve violence (i.e., assaults, etc.), reported missing persons, and reported runaways, will be created using photographs of those persons meeting the above criteria. The database may include persons meeting this criteria wanted by law enforcement agencies other than the Virginia Beach Police Department. Additionally, photographs of department personnel, city leaders, or citizen volunteers may be entered into the system with their permission to serve as a verification system. This database will be utilized with the Facial Recognition Technology (FRT) and the Oceanfront CCTV camera systems.

Personal images, with a minimum threshold of 14 match points, captured by the camera system will be compared to those in the database. Those individual images found to match a wanted person, runaway or missing person, or test subjects will be maintained until such time that the image no longer meets the above stated criteria. All other individual images will be immediately discarded.

2. Alert Procedures:

When the Camera Monitoring Officer (CMO) receives an alert of a possible hit, he will view the two (2) photographs displayed to confirm that the software has identified a subject within the database. The CMO shall maintain a CMO Monitor's Log that will be utilized to document any alerts that may be registered by the FRT system. This will include all hits, encounters and the final disposition of any encounters. In addition to this log, the CMO shall also complete a FRT Hit form in the event positive identification and an arrest is made based on the technology.

Upon visually confirming the photograph is a possible match, the CMO will determine the nature of the alert (i.e., wanted person, runaway, or missing person). Based on the nature of the alert, the CMO will simultaneously contact the nearest patrol officer and an On Duty First Line Supervisor and advise of the potential hit and the nature of the alert. Upon this notification the CMO shall implement the appropriate responses depicted as follows:

A. Wanted Persons - After confirming the hit, the CMO will notify the closest uniformed officers of the alert, description of the subject, the specific charges, and the direction of travel. The CMO will then immediately confirm the existence and location of the warrant/s. After confirming the existence and location of the warrant/s, the CMO will notify the responding officers of that information. While confirming the warrant/s, the CMO will also obtain any additional information that may assist responding officers and ensure their safety, the safety of the subject to be encountered, as well as any bystanders.

The responding officers will locate and approach the possible subject based on Reasonable Suspicion, and conduct an "investigatory" stop (Terry v Ohio). It is imperative that the officers remember that this encounter is for investigative purposes only and that the alert or hit with the FRT is not probable cause for an arrest. At the earliest opportunity, the officer(s) will provide the citizen with an explanation of why they were stopped.

The officer(s) will take the necessary investigative steps to determine if the subject is in fact wanted. If the officer(s) determine that the subject of their encounter is not wanted he will be given a brief explanation for the encounter and immediately released. If the subject is confirmed as being wanted, the subject will be immediately taken into custody in accordance with existing policy and procedures. The officers shall immediately notify a supervisor and the CMO of the final disposition of the encounter and the actions that were taken.

The arresting officers shall process the prisoner in accordance to existing policy and procedures and they shall fax a copy of the tracer report to the CMO for documentation purposes. The CMO shall complete a FRT Hit form documenting the encounter and arrest.

B. Runaways - After confirming the hit, the CMO will confirm the status of the runaway through NCIC and/or PISTOL. The CMO will also contact Juvenile Intake and confirm the existence of an active pick up order. The CMO will also request any additional information from the Intake worker that may assist and ensure the safety of the responding officers, bystanders, and the juvenile to be encountered.

The officers will approach the juvenile and using an investigatory stop, determine if the juvenile is in fact the runaway. If the juvenile is not the runaway and if there are no other underlying reason or causes for detention (curfew, etc.), the juvenile will be given a brief explanation for the encounter and released. If the juvenile is determined to be the runaway, they will be taken into custody in accordance with existing policies and procedures and transported to juvenile intake. The CMO and supervisor will be notified of the final disposition of the encounter. The CMO will document the encounter as described above with due regard to the juvenile status of the offender.

C. Missing Persons - The same procedures shall apply with the identifying and encounters of a missing person. The CMO after confirming the hit shall attempt to confirm the IBR (Incident Based Reporting) for missing persons and any other information such as medical condition or other factors. The responding officers shall conduct an investigatory stop to determine the identity of the subject and take the appropriate action. If the person approached is not the missing person, they will be given a brief explanation for the encounter and released. The supervisor and CMO will be notified of the final disposition of the encounter.

D. Federal Bureau of Investigation Terrorist Most Wanted List - The FBI maintains a list of subjects that are wanted for questioning or have active federal warrants on file, regarding terrorist activities and/or threats. Images of individuals on this list will be entered into the database with the appropriate FBI alerts and contact numbers. The CMO will check with the FBI on a daily basis to determine status of the individuals on the list and remove or enter images as required by this policy.

E. External Digitized Images - The Virginia Beach Police Department currently utilizes digital technology to capture digital video and still images by use of handheld video and still cameras. The use of this technology allows for more mobility, which furthers the capabilities of the Facial Recognition Technology. In the event that a subject meeting the criteria outlined in this policy is located outside of the viewing area of the fixed FRT cameras, their digital image may be captured by handheld digital recording devices and entered into the database for processing. If an alert is received, the proper response outlined in this policy will be implemented. In the event that there is no alert, the image will be immediately removed from both the FRT system as well as the recording media used to capture the image. The use and input of external digital images will only be

utilized with the approval of the Commanding Officer of the Second Police Precinct or the Commanding Officer of Special Investigations, or their designees.

Random external digitized images of persons and/or crowds will not be entered into the FRT, for any reason. A request for use of the FRT with external digital images, will be noted in the FRT log with the specific reason for the request. In addition, the CMO will complete the FRT Alert form.

3. CMO Alert/Encounter Logs:

The CMO will maintain a log for documenting all alerts and encounters that are a direct result of the FRT System. These logs will be reviewed on a weekly basis by the Second Precinct Lieutenant who shall submit a monthly report to the Chief of Police via the Chain of Command. These logs shall be maintained at the Second Police Precinct for three (3) years and shall be disposed of, in accordance with existing policies and procedures.

4. Systems Operation:

Under normal operations criteria, the CMO will ensure that the Facial Recognition System is operating in its automatic mode and receiving inputs from the two dedicated cameras. The CMO will not manually cause the system to target any individuals unless they are searching for a wanted person who has been specifically identified by citizens, a law enforcement officer, or other verifiable means, or missing persons who have been reported by citizens and/or police officers.

Under no circumstances will members of the CMO or any other Department member allow the system to be operated in a manner that could be construed or perceived as being discriminatory towards anyone based on race, gender, ethnicity, or any other non-criminal criteria.

5. Security:

There will be multiple layers of security, which prohibit unauthorized entry or removal of information from the database. Only sworn police officers specifically identified and authorized in writing by the Chief of Police shall have access to the database. The identified officers will have the sole responsibility for entering images into the database and ensuring that all those in the database meet the governing criteria on an ongoing basis. This will require constant verification of warrants and other investigative reporting for runaways and missing persons.

The system will also be password protected with only authorized officers possessing the password. As an additional level of security, the password will be changed at least every 180 days by the system administrator.

Finally, to ensure no unauthorized entry into the database, the system will be a stand-alone system and not connected to any LAN/WAN. Information in the database will not be shared with anyone without the expressed approval of the Chief of Police.

6. Entry/Validation:

The CMO will receive a daily report from Police Services listing all new felony warrants issued. After receiving the listing, the CMO will coordinate with Forensic Services Unit and/or the Sheriff's Department Central Booking Unit to determine if a photograph of the subject is available. If a photograph is available, it will be requested and entered into the system after the CMO ensures it meets all applicable criteria.

To ensure current and accurate data, the CMO will also receive a report daily from Police Services detailing the warrants served for the previous 24 hours. The CMO will compare the warrants served with the database to ensure that images of those individuals arrested are removed.

7. Audit:

The precinct lieutenant responsible for camera operations will conduct quarterly audits to ensure all policies and procedures concerning the Facial Recognition Technology System is functioning properly. A report of this audit will be provided to the Chief of Police and maintained in the grant documentation.

Additionally, random audits will be conducted by the Facial Recognition Program Citizen Advisory and Audit Committee. Between the dates of May 1st and September 30th, the Committee will conduct monthly audits. During the remaining months between October 1st and April 30th, the Committee will conduct quarterly audits. Committee members will have complete and open access to databases, alert/encounter logs, and any other documentation pertaining to the facial recognition program.

Members of the audit committee will provide a written report utilizing the Facial Recognition Audit Form outlining their findings, assessment, and recommendations to the Chief of Police within 48 hours of any audit/review they conduct. Copies of these reports will be maintained with other grant documentation and utilized during the ongoing evaluation process.

Appendix 7

Dissemination of Other States' Social Security Numbers Legislation

Arizona - Title 44, Chapter 9, Article 17 (§ 44-1373 et seq.)	California - Civil Code Section 1798.85-1798.86	Illinois - 815 ILCS 505 / 2QQ	Maryland (vetoed) - Senate Bill 117 (2004 Regular Session)
RESTRICTIONS A. Except as otherwise specifically provided by law, beginning on January 1, 2005, a person or entity shall not: **(note - applies to govt. in part, see below)**	**RESTRICTIONS** (a) Except as provided in subdivisions (b), (h), and (i), a person or entity may not do any of the following: **(note - applies to government)**	**RESTRICTIONS** (a) Except as otherwise provided in this Section, a person may not do any of the following: **(note - government is excluded below)**	**RESTRICTIONS** (A) Except as otherwise provided in this subtitle, a person may not: **(note - excludes state and local government)**
1. Intentionally communicate or otherwise make an individual's social security number available to the general public. **(note - individual is defined as resident of the state)**	(1) Publicly post or publicly display in any manner an individual's social security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public.	(1) Publicly post or publicly display in any manner an individual's social security number. As used in this Section, "publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public.	(1) Publicly post or display an individual's social security number; **(note - "Publicly post or display" means to intentionally communicate or otherwise make available to the general public.)**
2. Print an individual's social security number on any card required for the individual to receive products or services provided by the person or entity.	(2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity.	(2) Print an individual's social security number on any card required for the individual to access products or services provided by the person or entity; however, a person or entity that provides an insurance card must print on the card an identification number unique to the holder of the card in the format prescribed by Section 15 of the Uniform Prescription Drug Information Card Act.	(2) Print an individual's social security number on a card required for the individual to access products or services provided by the person;
3. Require the transmission of an individual's social security number over the Internet unless the connection is secure or	(3) Require an individual to transmit his or her social security number over the Internet unless the connection is secure or the social	(3) Require an individual to transmit his or her social security number over the Internet, unless the connection is secure or	(3) Require an individual to transmit the individual's social security number over the Internet unless the connection is secure or the social security number is

Arizona - Title 44, Chapter 9, Article 17 (§ 44-1373 et seq.)	California - Civil Code Section 1798.85-1798.86	Illinois - 815 ILCS 505 / 2QQ	Maryland (vetoed) - Senate Bill 117 (2004 Regular Session)
the social security number is encrypted.	security number is encrypted.	the social security number is encrypted.	encrypted;
4. Require the use of an individual's social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the site.	(4) Require an individual to use his or her social security number to access an Internet Web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.	(4) Require an individual to use his or her social security number to access an Internet web site, unless a password or unique personal identification number or other authentication device is also required to access the Internet Web site.	(4) Require an individual to use the individual's social security number to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the website; or
5. Print a number that the person or entity knows to be an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. This paragraph does not prohibit the mailing of documents that include social security numbers sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the social security number. In a transaction involving or otherwise relating to an individual, if a person or entity receives a number from a third party, the person or entity has no duty to inquire or otherwise determine if the number is or includes that individual's social security number. The person or entity may	(5) Print an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. Notwithstanding this paragraph, social security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the social security number. A social security number that is permitted to be mailed under this section may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened.	(5) Print an individual's social security number on any materials that are mailed to the individual, unless State or federal law requires the social security number to be on the document to be mailed. Notwithstanding any provision in this Section to the contrary, social security numbers may be included in applications and forms sent by mail, including documents sent as part of an application or enrollment process or to establish, amend, or terminate an account, contract, or policy or to confirm the accuracy of the social security number. A social security number that may permissibly be mailed under this Section may not be printed, in whole or in part, on a postcard or other mailer that does not require an envelope or be visible on an envelope or visible without the envelope	(5) Print an individual's social security number on any material that is mailed, electronically mailed, or transmitted by facsimile to the individual, unless required by state or federal law. **(Gov. vetoed the bill because this provision prevents email and fax.)** (B) This section does not apply to: (2) The inclusion of an individual's social security number in an application, form, or document sent by mail: (I) As part of an application or enrollment process; (II) To establish, amend, or terminate an account, contract, or policy; or (III) To confirm the accuracy of the individual's social security number; or

Arizona - Title 44, Chapter 9, Article 17 (§ 44-1373 et seq.)	California - Civil Code Section 1798.85-1798.86	Illinois - 815 ILCS 505 / 2QQ	Maryland (vetoed) - Senate Bill 117 (2004 Regular Session)
print that number on materials that are mailed to the individual, unless the person or entity that received the number has actual knowledge that the number is or includes the individual's social security number. This paragraph does not prohibit the mailing to the individual of any copy or reproduction of a document that includes a social security number if the social security number was included on the original document before January 1, 2005.		having been opened.	
CONTINUED USE B. Notwithstanding subsection A, a person or entity that before January 1, 2005 used an individual's social security number in a manner inconsistent with subsection a may continue using that individual's social security number in that manner on and after January 1, 2005 ***subject to the following conditions***: 1. The use of the social security number must be continuous. If the use is stopped for any reason, subsection A applies. 2. Beginning in 2005, the person or entity must provide the individual with an annual written disclosure of the individual's right to stop the use of the social	**CONTINUED USE** (b) Except as provided in subdivision (e), a person or entity that has used, prior to July 1, 2002, an individual's social security number in a manner inconsistent with subdivision (a), may continue using that individual's social security number in that manner on or after July 1, 2002, and a state or local agency that has used, prior to January 1, 2004, an individual's social security number in a manner inconsistent with subdivision (a), may continue using that individual's social security number in that manner on or after January 1, 2004, if all of the following conditions are met: (1) The use of the social	**CONTINUED USE** (b) A person that used, before July 1, 2005, an individual's social security number in a manner inconsistent with subsection (a) may continue using that individual's social security number in the same manner on or after July 1, 2005 if all of the following conditions are met: (1) The use of the social security number is continuous. If the use is stopped for any reason, subsection (a) shall apply. (2) The individual is provided an annual disclosure that informs the individual that he or she has the right to stop the use of his or her social security number in a manner prohibited	**CONTINUED USE** (Separate Section - expires on December 31, 2007) (A) A person that used an individual's social security number prior to January 1, 2005, in a manner prohibited under § 14-3202(a) of this subtitle may continue to use the individual's social security number in that manner ***if***: (1) The use of the individual's social security number is continuous; ***and*** (2) Beginning on January 1, 2005, the person provides the individual with an annual disclosure form stating the individual's right to stop the use of the individual's social security number in the manner prohibited under § 14-3202(a) of this subtitle. (b) (1) A written request by an individual to stop the use

Arizona - Title 44, Chapter 9, Article 17 (§ 44-1373 et seq.)	California - Civil Code Section 1798.85-1798.86	Illinois - 815 ILCS 505 / 2QQ	Maryland (vetoed) - Senate Bill 117 (2004 Regular Session)
security number in a manner prohibited by subsection A. 3. If the individual requests in writing, the person or entity must stop using the social security number in a manner prohibited by subsection a within thirty days after receiving the request. No fee or charge is allowed for implementing the request, and the person or entity shall not deny services to the individual because of the request.	security number is continuous. If the use is stopped for any reason, subdivision (a) shall apply. (2) The individual is provided an annual disclosure, commencing in the year 2002, that informs the individual that he or she has the right to stop the use of his or her social security number in a manner prohibited by subdivision (a). (3) A written request by an individual to stop the use of his or her social security number in a manner prohibited by subdivision (a) shall be implemented within 30 days of the receipt of the request. There shall be no fee or charge for implementing the request. (4) A person or entity, not including a state or local agency, shall not deny services to an individual because the individual makes a written request pursuant to this subdivision.	by subsection (a). A written request by an individual to stop the use of his or her social security number in a manner prohibited by subsection (a) shall be implemented within 30 days of the receipt of the request. There shall be no fee or charge for implementing the request. A person shall not deny services to an individual because the individual makes such a written request.	of the individual's social security number in a manner prohibited under § 14-3202(a) of this subtitle shall be implemented within 30 days after receipt of the request. (2) A person may not deny products or services to an individual because the individual makes a written request under this subsection.
LIMITATION C. This section does not prohibit the collection, use or release of a social security number as required by the laws of this state or the United States or for internal verification or administrative purposes.	**LIMITATION** (c) This section does not prevent the collection, use, or release of a social security number as required by state or federal law or the use of a social security number for internal verification or administrative	**LIMITATION** (c) This Section does not apply to the collection, use, or release of a social security number as required by State or federal law or the use of a social security number for internal	**LIMITATION** (B) This section does not apply to: (1) The collection, release, or use of an individual's social security number as required by state or federal law;

Arizona - Title 44, Chapter 9, Article 17 (§ 44-1373 et seq.)	California - Civil Code Section 1798.85-1798.86	Illinois - 815 ILCS 505 / 2QQ	Maryland (vetoed) - Senate Bill 117 (2004 Regular Session)
	purposes.	verification or administrative purposes.	(3) The use of an individual's social security number for internal verification or administrative purposes.
GOVERNMENT USE D. Beginning on January 1, 2005, this state or any political subdivision of this state shall not use an individual's social security number on state issued or political subdivision issued forms of identification. E. This section does not prohibit an agency of this state or a county, city, town or other political subdivision of this state from disseminating or using the last four numbers of an individual's social security number. F. A government agency shall not transmit to an individual material that contains both an individual's social security number and bank, savings and loan association or credit union account number. This paragraph does not prohibit the transmitting of documents that include social security and bank, savings and loan association or credit union account numbers as a part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the		**GOVERNMENT USE** This Section does not apply to the collection, use, or release of a social security number by the State, a subdivision of the State, or an individual in the employ of the State or a subdivision of the State in connection with his or her official duties.	

Arizona - Title 44, Chapter 9, Article 17 (§ 44-1373 et seq.)	California - Civil Code Section 1798.85-1798.86	Illinois - 815 ILCS 505 / 2QQ	Maryland (vetoed) - Senate Bill 117 (2004 Regular Session)
accuracy of the social security, bank, savings and loan association or credit union account number.			
EXEMPTIONS 44-1373.01. Exceptions This article does not apply to: 1. The use of social security numbers by the department of revenue or by a law enforcement agency of this state or a law enforcement agency of a county, city, town or other political subdivision of this state, except that these agencies must comply with section 44-1373, subsection A, paragraphs 2 and 5. 2. The use of social security numbers by an agency of this state in its administration of employee payroll, employee benefits and workers' compensation matters, except that the agency shall comply with section 44-1373, subsection A, paragraphs 1, 2, 4 and 5. 3. Documents or records that are recorded or required to be open to the public pursuant to the constitution or laws of this state or by court rule or order, and this article does not limit access to these documents or records.	**EXEMPTIONS** (d) This section does not apply to documents that are recorded or required to be open to the public pursuant to Chapter 3.5 (commencing with Section 6250), Chapter 14 (commencing with Section 7150) or Chapter 14.5 (commencing with Section 7220) of Division 7 of Title 1 of, or Chapter 9 (commencing with Section 54950) of Part 1 of Division 2 of Title 5 of, the Government Code. This section does not apply to records that are required by statute, case law, or California Rule of Court, to be made available to the public by entities provided for in Article VI of the California Constitution.	**EXEMPTIONS** (d) This Section does not apply to documents that are recorded or required to be open to the public under State or federal law, applicable case law, Supreme Court Rule, or the Constitution of the State of Illinois.	

Arizona - Title 44, Chapter 9, Article 17 (§ 44-1373 et seq.)	California - Civil Code Section 1798.85-1798.86	Illinois - 815 ILCS 505 / 2QQ	Maryland (vetoed) - Senate Bill 117 (2004 Regular Session)
4. An individual's social security number that is printed or caused to be printed on a document by the individual. 5. The use of social security numbers by the industrial commission of Arizona or an interested party as defined in section 23-901, on documents or records related to a workers' compensation claim under title 23, chapter 6, except that the industrial commission or the interested party shall comply with section 44-1373, subsection A, paragraphs 1, 2, 3 and 4.			
	INSURANCE PROVIDERS (e) (1) In the case of a health care service plan, a provider of health care, an insurer or a pharmacy benefits manager, a contractor as defined in Section 56.05, or the provision by any person or entity of administrative or other services relative to health care or insurance products or services, including third-party administration or administrative services only, this section shall become operative in the following manner: **(Note - Differentiate between new and renewing members and government run health plans as to date of effect.)**		**INSURANCE PROVIDERS** SECTION 3. AND BE IT FURTHER ENACTED, That this Act shall apply to all health insurance policies and contracts issued, delivered, or renewed in the State on or after January 1, 2005. Any health insurance policy or contract in effect before January 1, 2005, shall comply with the provisions of this Act on or before January 1, 2006.

Arizona - Title 44, Chapter 9, Article 17 (§ 44-1373 et seq.)	California - Civil Code Section 1798.85-1798.86	Illinois - 815 ILCS 505 / 2QQ	Maryland (vetoed) - Senate Bill 117 (2004 Regular Session)
	FEDERAL IDENTIFIER (f) If a federal law takes effect requiring the United States Department of Health and Human Services to establish a national unique patient health identifier program, a provider of health care, a health care service plan, a licensed health care professional, or a contractor, as those terms are defined in Section 56.05, that complies with the federal law shall be deemed in compliance with this section.	**FEDERAL IDENTIFIER** (e) If a federal law takes effect requiring the United States Department of Health and Human Services to establish a national unique patient health identifier program, any person who complies with the federal law shall be deemed to be in compliance with this Section.	
ADDITIONAL RESTRICTIONS 44-1373.02. Restricted use of sequential numbers; definition A. Except as otherwise specifically provided by law, beginning on January 1, 2009, a person or entity shall not knowingly: 1. Print any sequence of more than five numbers that are reasonably identifiable as being part of an individual's social security number on any card required for the individual to receive products or services provided by the person or entity. 2. Print any sequence of more than five numbers that are reasonably	**ADDITIONAL RESTRICTIONS** (g) A person or entity may not encode or embed a social security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the social security number, as required by this section.	**ADDITIONAL RESTRICTIONS** (f) A person may not encode or embed a social security number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the social security number as required by this Section.	

Arizona - Title 44, Chapter 9, Article 17 (§ 44-1373 et seq.)	California - Civil Code Section 1798.85-1798.86	Illinois - 815 ILCS 505 / 2QQ	Maryland (vetoed) - Senate Bill 117 (2004 Regular Session)
identifiable as being part of an individual's social security number on any materials that are mailed to the individual, unless state or federal law requires the social security number to be on the document to be mailed. This paragraph does not prohibit the mailing of documents to the individual that include social security numbers or any sequence of numbers contained in a social security number that is sent as part of an application or enrollment process or to establish, amend or terminate an account, contract or policy or to confirm the accuracy of the social security number or sequence of numbers. B. "Individual" means a resident of this state.			
	ADDITIONAL PROVISIONS Additional provisions stating when the law takes effect for various government entities. 1798.86. Any waiver of the provisions of this title is contrary to public policy, and is void and unenforceable.	**ADDITIONAL PROVISIONS** (g) Any person who violates this Section commits an unlawful practice within the meaning of this Act.	**ADDITIONAL PROVISIONS** Violation of these provisions is also considered a deceptive trade practice in violation of the Consumer Protection Law.

Michigan - Chapter 445 Trade & Commerce (§ 445.81, et seq)	Missouri - Title XXVI, Chapter 407 (§ 407.1355.1)	Texas - Business and Commerce Code Section, Title 4, Chapter 35 (§ 35.58)
RESTRICTIONS (1) Except as provided in	**RESTRICTIONS** A person or entity, not including a state	**RESTRICTIONS** (a) A person, other than

Michigan - Chapter 445 Trade & Commerce (§ 445.81, et seq)	Missouri - Title XXVI, Chapter 407 (§ 407.1355.1)	Texas - Business and Commerce Code Section, Title 4, Chapter 35 (§ 35.58)
subsection (2), a person shall not intentionally do any of the following with the social security number of an employee, student, or other individual: **(note - person includes all legal entities, including government)**	or local agency, shall not do any of the following:	government or a governmental subdivision or agency, may not:
(a) Publicly display all or more than 4 sequential digits of the social security number. **(note - "Publicly display" means to exhibit, hold up, post, or make visible or set out for open view, including, but not limited to, open view on a computer device, computer network, website, or other electronic medium or device, to members of the public or in a public manner. The term does not include conduct described in … (1)(b), (c), or (f).)**	(1) Publicly post or publicly display in any manner an individual's Social Security number. "Publicly post" or "publicly display" is defined in this section to intentionally communicate or otherwise make available to the general public;	(1) Intentionally communicate or otherwise make available to the general public an individual's social security number;
(b) Subject to subsection (3), use all or more than 4 sequential digits of the social security number as the primary account number for an individual. However, if the person is using the social security number under subdivision (c) and as the primary account number on the effective date of this act, this subdivision does not apply to that person until January 1, 2006. (c) Visibly print all or more than 4 sequential digits of the social security number on any identification badge or card, membership card, or permit or license. However, if a person has implemented or implements a plan or schedule that establishes a specific date by which it will comply with this subdivision, this subdivision does not apply to that person until January 1, 2006, or the completion date specified in that plan or schedule, whichever is earlier.		(2) Display an individual's social security number on a card or other device required to access a product or service provided by the person;
(d) Require an individual to use or	(2) Require an individual to transmit	(3) Require an individual to

Michigan - Chapter 445 Trade & Commerce (§ 445.81, et seq)	Missouri - Title XXVI, Chapter 407 (§ 407.1355.1)	Texas - Business and Commerce Code Section, Title 4, Chapter 35 (§ 35.58)
transmit all or more than 4 sequential digits of his or her social security number over the internet or a computer system or network unless the connection is secure or the transmission is encrypted.	his or her Social Security number over the Internet, unless the connection is secure or the Social Security number is encrypted;	transmit the individual's social security number over the Internet unless the connection is secure or the number is encrypted;
(e) Require an individual to use or transmit all or more than 4 sequential digits of his or her social security number to gain access to an internet website or a computer system or network unless the connection is secure, the transmission is encrypted, or a password or other unique personal identification number or other authentication device is also required to gain access to the internet website or computer system or network.	(3) Require an individual to use his or her Social Security number to access an Internet web site, unless a password, unique personal identification number, or other authentication device is also required to access the Internet website.	(4) Require an individual's social security number for access to an Internet website, unless a password or unique personal identification number or other authentication device is also required for access; or
(f) Include all or more than 4 sequential digits of the social security number in or on any document or information mailed or otherwise sent to an individual if it is visible on or, without manipulation, from outside of the envelope or packaging. (g) Subject to subsection (3), beginning January 1, 2006, include all or more than 4 sequential digits of the social security number in any document or information mailed to a person, unless any of the following apply: (i) State or federal law, rule, regulation, or court order or rule authorizes, permits, or requires that a social security number appear in the document. (ii) The document is sent as part of an application or enrollment process initiated by the individual. (iii) The document is sent to		(5) Print an individual's social security number on any materials, except as provided by Subsection (f) that are sent by mail, unless state or federal law requires that the individual's social security number be included in the materials. (f) Subsection (a)(5) does not apply to an application or form sent by mail, including a document sent: (1) as part of an application or enrollment process; (2) to establish, amend, or terminate an account, contract, or policy; or (3) to confirm the accuracy of a social security number.

Michigan - Chapter 445 Trade & Commerce (§ 445.81, et seq)	Missouri - Title XXVI, Chapter 407 (§ 407.1355.1)	Texas - Business and Commerce Code Section, Title 4, Chapter 35 (§ 35.58)
establish, confirm the status of, service, amend, or terminate an account, contract, policy, or employee or health insurance benefit or to confirm the accuracy of a social security number of an individual who has an account, contract, policy, or employee or health insurance benefit. (iv) The document or information is mailed by a public body under any of the following circumstances: (A) The document or information is a public record and is mailed in compliance with the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246. (B) The document or information is a copy of a public record filed or recorded with a county clerk or register of deeds office and is mailed by that office to a person entitled to receive that record. (C) The document or information is a copy of a vital record recorded as provided by law and is mailed to a person entitled to receive that record. (v) The document or information is mailed by or at the request of an individual whose social security number appears in the document or information or his or her parent or legal guardian. (vi) The document or information is mailed in a manner or for a purpose consistent with subtitle A of title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809; with the health insurance portability and accountability act of 1996, Public Law 104-191; or with section 537 or 539 of the		

Michigan - Chapter 445 Trade & Commerce (§ 445.81, et seq)	Missouri - Title XXVI, Chapter 407 (§ 407.1355.1)	Texas - Business and Commerce Code Section, Title 4, Chapter 35 (§ 35.58)
insurance code of 1956, 1956 PA 218, MCL 500.537 and 500.539.		
CONTINUED USE (3) It is not a violation of subsection (1)(b **- account number**) or (g **- mailing**) to use all or more than 4 sequential digits of a social security number if the use is any of the following: (b) A use of all or more than 4 sequential digits of a social security number as a primary account number that meets both of the following: (i) The use began before the effective date of this act **(March 1, 2005)**. (ii) The use is ongoing, continuous, and in the ordinary course of business. If the use is stopped for any reason, this subdivision no longer applies.	**CONTINUED USE** 2. Except as provided in subsection 3 of this section, the provisions of subsection 1 of this section apply only to the use of Social Security numbers on or after July 1, 2006. 3. Except as provided in subsection 6 of this section, a person or entity, not including a state or local agency, that has used, prior to July 1, 2006, an individual's Social Security number in a manner inconsistent with subsection 1 of this section may continue using that individual's Social Security number in that manner on or after July 1, 2006, ***if any*** of the following conditions are met: (1) The use of the Social Security number is continuous. If the use is stopped for any reason, subsection 1 of this section shall apply; (2) The individual is provided an annual disclosure, beginning in 2006, that informs the individual that he or she has the right to stop the use of his or her Social Security number in a manner prohibited by subsection 1 of this section; or (3) A written request by an individual to stop the use of his or her Social Security number in a manner prohibited by subsection 1 of this section shall be implemented within thirty days of the receipt of the request. There shall be no fee or charge for implementing the request. A person or entity, not including a state or local agency, shall not deny services to an individual because the individual makes a written request pursuant to this subdivision.	**CONTINUED USE** (b) A person that is using an individual's social security number before January 1, 2005, in a manner prohibited by subsection (a) may continue that use if: (1) the use is continuous; and (2) the person provides annual disclosure to the individual, beginning January 1, 2006, stating that on written request from the individual the person will cease to use the individual's social security number in a manner prohibited by subsection (a). (c) A person, other than government or a governmental subdivision or agency, may not deny services to an individual because the individual makes a written request under Subsection (b). (d) If a person receives a request from an individual directing the person to stop using the individual's social security number in a manner prohibited by Subsection (a), the person shall comply with the request not later than the 30th day after the date the request is received. The person may not impose a fee or charge for complying with the request.
LIMITATION (2) Subsection (1) does not apply to any of the following:	**LIMITATION** 4. This section does not prevent the collection, use, or release of a Social	**LIMITATION** (e) This section does not apply to:

Michigan - Chapter 445 Trade & Commerce (§ 445.81, et seq)	Missouri - Title XXVI, Chapter 407 (§ 407.1355.1)	Texas - Business and Commerce Code Section, Title 4, Chapter 35 (§ 35.58)
(a) A use of all or more than 4 sequential digits of a social security number that is authorized or required by state or federal statute, rule, or regulation, by court order or rule, or pursuant to legal discovery or process. (3) It is not a violation of subsection (1)(b) or (g) to use all or more than 4 sequential digits of a social security number if the use is any of the following: (a) An administrative use of all or more than 4 sequential digits of the social security number in the ordinary course of business, by a person or a vendor or contractor of a person, to do any of the following: (i) Verify an individual's identity, identify an individual, or do another similar administrative purpose related to an account, transaction, product, service, or employment or proposed account, transaction, product, service, or employment. (ii) Investigate an individual's claim, credit, criminal, or driving history. (iii) Detect, prevent, or deter identity theft or another crime. (iv) Lawfully pursue or enforce a person's legal rights, including, but not limited to, an audit, collection, investigation, or transfer of a tax, employee benefit, debt, claim, receivable, or account or an interest in a receivable or account. (v) Lawfully investigate, collect, or enforce a child or spousal support obligation or tax liability.	Security number as required by state or federal law or the use of a Social Security number for internal verification or administrative purposes.	(1) the collection, use, or release of a social security number that is required by state or federal law, including Chapter 552, Government Code; or (2) the use of a social security number for internal verification or administrative purposes;

Michigan - Chapter 445 Trade & Commerce (§ 445.81, et seq)	Missouri - Title XXVI, Chapter 407 (§ 407.1355.1)	Texas - Business and Commerce Code Section, Title 4, Chapter 35 (§ 35.58)
(vi) Provide or administer employee or health insurance or membership benefits, claims, or retirement programs or to administer the ownership of shares of stock or other investments.		
GOVERNMENT USE (2) Subsection (1) does not apply to any of the following: (b) A use of all or more than 4 sequential digits of a social security number by a title IV-D agency, law enforcement agency, court, or prosecutor as part of a criminal investigation or prosecution, or providing all or more than 4 sequential digits of a social security number to a title IV-D agency, law enforcement agency, court, or prosecutor as part of a criminal investigation or prosecution.		
EXEMPTIONS Sec. 5. All or more than 4 sequential digits of a social security number contained in a public record are exempt from disclosure under the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246, pursuant to section 13(1)(d) of the freedom of information act, 1976 PA 442, MCL 15.243.	**EXEMPTIONS** 5. This section does not apply to documents that are recorded or required to be open to the public pursuant to chapter 610, RSMo. This section does not apply to records that are required by statute, case law, or Missouri court rules to be made available to the public.	**EXEMPTIONS** (3) documents that are recorded or required to be open to the public under Chapter 552, Government Code; (4) court records; or (5) an institution of higher education if the use of a social security number by the institution is regulated by Chapter 51, Education Code, or another provision of the Education Code.
INSURANCE PROVIDERS		
	FEDERAL IDENTIFIER 6. If a federal law takes effect requiring the United States Department of Health and Human Services to establish a national unique patient health identifier program, any person or entity that complies with the federal law shall be deemed in compliance with this section.	
ADDITIONAL PROVISIONS		

Michigan - Chapter 445 Trade & Commerce (§ 445.81, et seq)	Missouri - Title XXVI, Chapter 407 (§ 407.1355.1)	Texas - Business and Commerce Code Section, Title 4, Chapter 35 (§ 35.58)
Sections 1 and 2 name the Act and define terms. Section 4 requires persons who obtain 1 or more social security numbers in the ordinary course of business to create and publish a privacy policy with specific requirements by January 1, 2006. This sections excludes entities required to comply with the Fair Credit Reporting Act and Gramm-Leach-Bliley Act. Section 6 provides criminal penalties and civil actions. Section 7. Effective March 1, 2005.		

Appendix 8

2005 LEGISLATION WITH TECHNOLOGY OR SCIENCE CONTENT
(ARRANGED BY SUBJECT MATTER)

Legislation recommended by the Joint Commission on Technology and Science is in **bold.**
Passed legislation is *italicized*.
Bills carried over from the 2004 Session that failed in 2005 are not included in this appendix.

Commerce

HB 1571	Entrepreneurial Encouragement Program; created for start-up businesses.
HB 1572	Venture capital funds; creation of an investment program.
HB 1692	Technology and Biotechnology Research and Development Fund; created.
HB 1804	Voice-over-Internet protocol service; exempt from regulation by State Corporation Commission.
HB 1864	Payday loans; use of Internet database for borrowers, rollovers prohibited by lenders.
HB 1948	*Administrative Process Act; impact on small businesses.*
HB 2033	*Semiconductor manufacturing performance grants; updates to make a qualified manufacturer eligible.*
HB 2055	*Telephone Privacy Protection Act; prohibits telephone solicitation, date change made consistent with federal regulations.*
HB 2057	Retail Sales and Use Tax; exemptions include telecommunication and telephone companies.
HB 2115	Administrative Process Act; impact on small businesses.
HB 2180	Solar energy devices; prohibits imposition of covenants that unreasonably limit installation.
HB 2218	*Gift certificate disclosures; definition, penalty.*
HB 2285	Fax machines; identification of sender of advertising materials.
HB 2467	Online Dating Safety Act; created.
HB 2880	*Communications services; various revisions to taxation thereof.*
HB 2889	Retail Sales & Use Tax; exemptions include public service corporation, telecommunications & telephone companies.
HB 2893	Telework Council; created, telecommuting tax credits for certain employers.
HJ 588	*Stem cell research; joint subcommittee to study medical, ethical & scientific issues relating to.*
HJ 598	*Biodiesel fuel use and production; Sec. of Agriculture & Forestry to study use & production thereof.*
HJ 813	NASA exploration program; urging Congress to enact and fully fund proposed vision therefore.
HR 29	Excise tax, federal; urging Congress to repeal on telecommunications.
SB 776	*Banks; prohibits unauthorized use of name, logo, etc., penalty.*

SB 912 *Consumer Protection Act; reduces punitive damage that may be awarded upon finding willful violation.*

SB 1116 Retail Sales and Use Tax; exemptions include telecommunication and telephone companies.

SB 1241 *Gift certificates; minimum term and disclosures.*

SB 1317 Cell phones; retailer to have recycling system for acceptance and collection of used.

Criminal Law and the Courts

HB 578 *Use of electronic communication for certain filings; parties and witnesses*.

HB 1639 Felonies; DNA analysis of arrestees for solicitation of prostitution or drug offense.

HB 1696 Harassment with a camera; penalty.

HB 1706 *Fees collected by clerks of circuit courts; use thereof.*

HB 1707 Commission on the Offices of the Clerks of the Circuit Courts; created, reports.

HB 1729 Computer Crimes Act; prohibited software and actions.

HB 1741 *Filming, videotaping or photographing of another; penalty when permission not given.*

HB 1799 Criminal history records; dissemination of information.

HB 1860 *Credit cards or numbers; unauthorized possession of two or more.*

HB 1871 Computer crimes; changes in provisions, penalties.

HB 1959 Fees; fixed cost for court copies needed by low-income persons.

HB 2059 *Credit cards; unlawful use of scanning devices and re-encoders, penalty.*

HB 2214 Computer crimes; punishment for interfering with computer systems, penalty.

HB 2215 *Computer Crimes Act; changes in provisions, penalty.*

HB 2273 *Hunting; prohibits device/service that remote controls firearms, etc. to hunt birds, etc., penalty.*

HB 2304 Computer crimes; gathering personal information by deception (phishing), penalty.

HB 2353 Facial recognition technology; definition, regulations of use.

HB 2471 ***Computer Crimes Act; changes in provisions, penalty.***

HB 2472 **Computer Crimes Act; prohibited actions, penalty.**

HB 2473 **Computer Crimes Act; criminalizing hacking; penalty.**

HB 2631 *Computer crimes; changes in provisions, penalties.*

HB 2869 *Location and jurisdiction of wiretaps.*

SB 902 *Commission on Offices of the Clerks of Circuit Courts; created.*

SB 927 Destruction of court records.

SB 1001 *Computer crimes; punishment for interfering with computer systems, penalty.*

SB 1002 *Computer crimes; changes in provisions, penalties.*

SB 1021 Foreign orders; records from electronic communication service providers.

SB 1083 *Hunting; prohibits device/service that remote controls firearms, etc. to hunt birds, etc., penalty.*

SB 1147 *Computer crimes; gathering personal information by deception (phishing), penalty.*

SB 1163 *Computer Crimes Act; reduces thresholds for damages and punishment.*

SB 1192 *Personal information; prohibits posting certain on Internet.*

Privacy and Identity Theft

HB 2052 ***Clerks of court; prohibits posting personal information on Internet.***

HB 2134 Recording devices in motor vehicles; ownership of data.

HB 2135 Motor vehicle insurance; prohibits insurers from including in policy access to recorded data, penalty.

HB 2468 **Event data recorders in motor vehicles; manufacturers to disclose.**

HB 2469 Recording devices in motor vehicles; access to data.

HB 2474 Consumer Protection Act; restricting use of social security numbers.

HB 2482 ***Personal Information Privacy Act; restricting use of social security numbers.***

HB 2721 Personal Information Privacy Act; notification when database breach containing personal information has occurred.

HJ 691 Biometric identifiers; DMV, et al, to study feasibility of integration for driver's licenses, etc.

HJ 714 Study; contents of driver's licenses and special identification cards; report.

SB 998 Clerks of court; prohibits posting personal information on Internet.

State and Local Government

Local Government

HB 2158 *Wireless Service Authority; allows multiple localities & regional industrial facilities to create.*

HB 2395 Wireless Service Authorities; issuance of certificate of charter.

HB 2470 *Uniform Electronic Transactions Act; to include locally elected constitutional officers.*

HB 2534 Video Infrastructure Development and Competition Act of 2005; created.

HB 2797 Library computers; juveniles' Internet access.

HJ 788 *Commending the Central Virginia Governor's School for Science and Technology.*

SB 882 Library computers; juveniles' Internet access.

SB 960 Telecommunications services provided by localities; cost allocations.

SB 1337 Video infrastructure development; equalizing franchise requirements for competitors.

Procurement

HB 1945 *Public-Private Education Facilities and Infrastructure Act of 2002; definition of qualifying project.*

HB 2051 ***Public Procurement Act; purchase of technology, etc. to be approved by Chief Information Officer of State.***

HB 2054 ***Alternative, pilot project; VITA to study.***

HB 2151 *Public Procurement Act; preference for contractor firms.*

HB 2351 Small, women- and minority-owned businesses (SWAM); definition and regulations.

HB 2397 Procurement Act, Public; contracts with only U.S. citizens, legal aliens, etc.

HB 2419 Procurement Act, Public; contracts with only U.S. citizens, legal aliens, etc.

HB 2495 Procurement Act, Public; contracts with only U.S. citizens, legal aliens, etc.

HB 2844 *Competitive Government Act; change in reporting dates.*

HB 2845 Small businesses; encourages participation in state procurement transactions.
HB 2908 Procurement Act, Public; contracts with only U.S. citizens, legal aliens, etc.
HB 2924 Public Procurement Act; exemption from competitive sealed bidding and competitive negotiation.
SB 1286 Public Procurement Act; prohibited contracts; required contract provisions.

State Government

HB 1549 Electronic voting systems; to be equipped with voter-verified paper ballots.
HB 1661 State agencies; Governor to initiate financial and management review thereof.
HB 1691 Research and Technology Advisory Commission; membership.
HB 1733 Freedom of Information Act; exempts certain email addresses.
HB 1773 Absentee ballots; applications may be made on line.
HB1791 Virginia Public Records Act.
HB 1801 Biotechnology Research Partnership Authority; creates panel to make decisions about investments.
HB 2032 Powers and duties of Department of Emergency Management; Freedom of Information Act.
HB 2127 State agencies; establishment of telecommuting policy.
HB 2216 Department of Forensic Science, the Forensic Science Board, Scientific Advisory Board; created.
HB 2321 Reporting requirements of certain agencies and collegial bodies.
HB 2324 Educational Ventures Consortium; created.
HB 2404 Freedom of Information Act; exempts certain local wireless service authorities.
HB 2519 Immunization Information System (VIIS); established.
HB 2556 State agencies; Department of General Services to require services to be procured from private sectors.
HB 2560 Electronic voting systems; to be equipped with paper copy record of votes.
HB 2586 Technology and Science, joint commission on; clarifications for collegial bodies, report.
HB 2612 State employees; establishment of alternative work schedules and telecommuting.
HB 2672 Freedom of Information Act; exempts certain meetings from public disclosure.
HB 2753 Research and Technology Advisory Commission; membership
HB 2760 Freedom of Information Act; allows localities to conduct electronic meetings.
HB 2860 Innovative Technology Authority; repeals requirement to establish technical advisory committee.
HB 2913 Hydrogen Energy Plan; Secretary of Technology to develop, report.
HJ 647 Commending the Virginia Electronic Commerce Technology on its 10th anniversary.
HJ 711 Hydrogen Energy Plan; General Assembly to express its support therefor.
HJ 763 A. L. Philpott Manufacturing Extension Partnership (VPMEP); study ways to strengthen affiliation.
HR 27 House of Delegates; procedures governing live television coverage of sessions.
SB 711 Freedom of Information Act; changes for electronic communication meetings.
SB 752 University of Virginia; extends sunset provision for electronic meetings of Board of Visitors.

SB 808 Evidence, human biological; Division of Forensic Science to store, etc. & to develop inventory.
SB 879 Freedom of Information Act; exempts proprietary records of cable television, etc.
SB 934 *Public Accounts, Auditor of; duties.*
SB 938 Advisory boards, committees & commissions; removes limits on compensation & number of meetings.
SB 959 *Telecommunications and cable television; release of information (FOIA).*
SB 963 *Statewide communications interoperability; office of Governor to review & make recommendations.*
SB 992 *Uniform Real Property Electronic Recording Act; created.*
SB 1027 *Information Providers Network; change in authority.*
SB 1053 Higher educational institutions; intellectual property policies.
SB 1132 *Immunization Information System (VIIS); established.*
SB 1135 Retail Sales & Use Tax Act; renamed Streamlined Sales and Use Tax Agreement.
SB 1148 *Research and Technology Advisory Commission; membership.*
SB 1159 *Wireless E-911 Services Board; changes in provisions.*
SB 1194 *Christopher Reeve Stem Cell Research Fund; created.*
SB 1196 ***Freedom of Information Act; change in regulations for electronic communication meetings.***
SB 1249 Information Technology Investment Board; designating Secretary of Technology as chairperson.
SB 1252 Databases; changes requirement for periodic security audits of government.
SB 1262 Learning Technology, Office of; created within Council of Higher Education.
SB 1335 Communications services; various revisions to taxation thereof.
SJ 406 *Hydrogen energy.*
SJ 412 *Confirming Governor's appointments; administration.*
SJ 414 *Confirming Governor's appointments; commerce and trade.*
SJ 420 *Confirming Governor's appointments; technology.*
SJ 422 *Confirming Governor's appointments; miscellaneous positions.*

Transportation and Motor Vehicles

HB 1558 Traffic signals; use of photo-monitoring in certain localities.
HB 1630 VASCAR speed determination devices; allows City of Charlottesville to use.
HB 1830 Cell phones; prohibits use while driving.
HB 1868 Traffic signals; extends sunset on use of photo-monitoring systems, report.
HB 1962 Cell phones; prohibits use while driving.
HB 1983 *Video display in motor vehicles; prohibits in view of driver.*
HB 2095 Traffic signals; extends sunset on use of photo-monitoring systems.
HB 2105 Traffic signals; use of photo-monitoring systems in any locality.
HB 2274 Traffic signals; use of photo-monitoring in certain localities.
HB 2293 Motor vehicle titles; allows creation of electronic certificates of title.
HB 2389 Traffic signals; use of photo-monitoring in Williamsburg and James City County.
HB 2508 *Electronic summons; allows use for reportable motor vehicle violations.*
HJ 689 *Toll collections; Joint Comm. on Technology & Science to study technologies available therefor.*
SB 721 Traffic signals; use of photo-monitoring in Roanoke City.

SB 732	Traffic signals; use of photo-monitoring systems in any locality.
SB 780	Traffic signals; extends sunset on use of photo-monitoring systems.
SB 815	*Toll facilities; use of photo-monitoring systems.*
SB 1004	Traffic signals; use of photo-monitoring systems in any locality.
SB 1081	Cell phones; prohibits use of handheld devices while driving, except in emergency.
SB 1095	Traffic signals; abolishes sunset on use of photo-monitoring systems.

Appendix 9

Final Summaries of 2005 Enacted Legislation with Technology or Science Content

(In Numerical Order by HBs, HJRs, SBs and SJRs)

Full Text of Legislation Appears in the 2005 Acts of Assembly

HB 578 (Hamilton)

Use of electronic communication for certain filings; parties and witnesses. Provides that petitions and orders for emergency custody, temporary detention, and involuntary commitment of minors may be filed, issued, served, or executed by electronic means, with or without the use of two-way electronic video and audio communication. The bill also allows petitions and orders for emergency custody of adults, temporary detention of adults, emergency custody and temporary detention of adults in judicial authorization of treatment proceedings, and emergency custody of conditionally released persons to be filed, issued, served, or executed by electronic means, with or without the use of two-way electronic video and audio communication. The bill provides for party and witness testimony through two-way electronic video and audio communication in such proceedings. Finally, the bill allows a witness to testify using a telephonic communication system when his testimony would be helpful to the conduct of such proceedings and he is not able to be physically present.

HB 1691 (Purkey)

Virginia Research and Technology Advisory Commission; membership. Increases from 29 to 31 the membership of the Virginia Research and Technology Advisory Commission by adding the Vice-Provost of Research at the Eastern Virginia Medical School or his designee and one citizen member representing research- and technology-intensive industries appointed by the Governor. The bill also contains technical amendments.

HB 1706 (Kilgore)

Fees collected by clerks of circuit courts; authorization to use funds for office expenses. Provides that court clerks shall use the fees paid for copying to recoup the costs of providing the copies, with the balance of the funds paid to the Commonwealth. Funds sufficient to recoup the cost of making copies shall be deposited with the locality, which shall in turn appropriate funds to support copying costs. Such costs shall include lease and maintenance agreements, but shall not include salaries or related benefits.

HB 1741 (Cosgrove)

Photographs of undergarments, etc., without consent; penalty. Provides that the knowing and intentional creation of a videotape, photograph, film or videographic or still image record created by placing the lens or image-gathering component of a recording device directly beneath or between a person's legs for the purpose of capturing an image of the person's undergarments or intimate parts, when the undergarments or intimate parts would not otherwise be visible to the general public, is punishable as a Class 1 misdemeanor. The offense is punishable as a Class 6 felony if the nonconsenting person is under the age of 18.

HB 1791 (Cox)

Virginia Public Records Act. Makes several clarifying and technical changes to the Virginia Public Records Act. The bill removes obsolete definitions, clarifies existing definitions of "archival records" and "public records," and creates a definition for "private record," a term that is used in the Act but not currently defined. The bill removes references to the preservation of medical records, an area of law that has been superseded by other state and federal medical records laws, and programs for microfilming records by The Library of Virginia, a service not provided by The Library of Virginia. The bill also clarifies that a public record may not be destroyed or discarded unless certain requirements are met. This change codifies current practice. This bill is a recommendation of the HJR 6 study (2004).

HB 1801 (Watts)

Virginia Biotechnology Research Partnership Authority; Biotechnology Macro Partnership. Creates a panel to make decisions about the Commonwealth's biotechnology investments, upon implementation of any statewide program, referred to as the Virginia Biotechnology Macro. Certain provisions of the bill will expire on July 1, 2010.

HB 1860 (Shannon)

Unauthorized possession of two or more signed credit cards or credit card numbers. Clarifies that possession of two unauthorized credit cards is credit card theft and not forgery.

HB 1945 (Saxman)

Public-Private Education Facilities and Infrastructure Act of 2002; definition of qualifying project. Expands the definition of "qualifying project" to include any improvements necessary or desirable to any unimproved state or locally owned real estate.

HB 1948 (Saxman)

Administrative Process Act; impact on small businesses. Requires the Department of Planning and Budget, in addition to the economic impact analysis it already prepares concerning a proposed regulation, to differentiate between small businesses and other businesses identified; estimate the projected reporting, recordkeeping and other administrative costs required for compliance by such small businesses with the regulation; and include a description of any alternative method for achieving the purpose of the regulation while minimizing adverse impact on small businesses. The bill defines "small business" as a business entity, including its affiliates, that (i) is independently owned and operated and (ii) employs fewer than 500 full-time employees or has gross annual sales of less than $6 million. The bill also requires agencies to

periodically review their regulations to minimize the economic impact on small businesses.

HB 1983 (Howell, A.T.)

Video displays in motor vehicles. Prohibits drivers of motor vehicles from viewing any motion picture or video display while driving.

HB 2032 (Miles)

Powers and duties of Department of Emergency Management; coordination of emergency services intelligence and response; Freedom of Information Act. Provides that the Department of Emergency Management shall be responsible for the coordination, receipt, evaluation, and dissemination of emergency services intelligence and shall coordinate intelligence activities with the Department of State Police. The bill also creates a records exemption under the Virginia Freedom of Information Act for contact information, computer information, and operating schedule information submitted by an individual or agency for participation in the Statewide Alert Network where the release of such information would compromise the security of the Statewide Alert Network or individuals participating in the Statewide Alert Network.

HB 2033 (Miles)

Semiconductor manufacturing performance grants. Updates the Semiconductor Memory or Logic Wafer Manufacturing Performance Grant Program to make a qualified manufacturer eligible for total grant payments of up to $27 million if certain investment and job creation criteria are met. The measure also updates the Semiconductor Memory or Logic Wafer Manufacturing Performance Grant Program II to make a qualified manufacturer eligible for grant payments of (i) $15 million if $1.1 billion of new capital investment is made by January 1, 2007, that results in the creation of a new manufacturing module in Henrico County; (ii) $35 million if an additional 1,000 new full-

time jobs are created by January 1, 2008; and (iii) $5 million if 200 new full-time jobs are created by January 1, 2009.

HB 2051 (Nixon)

Virginia Public Procurement Act; methods of procurement. Requires approval of the Chief Information Officer of the Commonwealth for the purchase of information technology and telecommunications goods and services from a public auction or off of another public body's contract. The bill also provides that its provisions do not in any way amend or affect (i) the Commonwealth's institutions of higher education as such institutions are delegated the authority to purchase information technology facilities and services pursuant to any appropriation act adopted by the General Assembly or (ii) delegations of telecommunications procurement granted by the Virginia Information Technologies Agency.

HB 2052 (Nixon)

Clerks of court; posting certain information on the Internet; prohibitions. Extends the sunset clause prohibiting clerks from posting certain information on a court-controlled website from July 1, 2005, to July 1, 2007. Circuit court clerks are immunized against suit arising from any acts or omissions related to providing remote access on the Internet so long as the clerk was not grossly negligent and did not engage in willful misconduct.

HB 2054 (Nixon)

Alternative Dispute Resolution; pilot project. Allows the Virginia Information Technologies Agency (VITA) to promulgate administrative rules concerning the use of alternative dispute resolution in lieu of the provisions set forth in the Virginia Public Procurement Act concerning procurement protests. The Chief Information Officer of the Commonwealth must report to the General Assembly on the implementation of the rules. The pilot project will expire on July 1, 2008.

HB 2055 (Nixon)

Virginia Telephone Privacy Protection Act; telephone solicitation. Provides that telephone solicitors using a version of the National Do Not Call Registry obtained from their administrator no more than 31 days prior to the date of a telephone solicitation call constitutes a reasonable practice and procedure to effectively prevent telephone solicitation calls that would violate the Virginia Telephone Privacy Protection Act. The establishment and implementation of reasonable practices and procedures to effectively prevent such telephone solicitation calls is an affirmative defense to an action claiming a violation of the Act. Currently, such defense is available to telephone solicitors that use a version of the National Do Not Call Registry obtained within three months preceding the date of the call. Reducing the period from three months to 31 days makes the Act consistent with federal regulations.

HB 2059 (Byron)

Unlawful use of payment card scanning devices and re-encoders; penalty. Punishes as a Class 1 misdemeanor the malicious and unauthorized use of a scanner or re-encoder to unlawfully reproduce the information in the magnetic stripe of a payment card and as a Class 6 felony if the person sells or distributes such information to another or uses the information in the commission of another crime.

HB 2151 (Amundson)

Virginia Public Procurement Act; preference for Virginia firms. Provides that whenever the lowest responsive and responsible bidder is a resident of any other state and such state under its laws allows a resident contractor of that state a preference, a like preference shall be allowed to the lowest responsible bidder who is a resident of Virginia. The bill provides if the lowest bidder is a resident of another state with an absolute preference, that bid shall not be considered. Currently, a preference for Virginia resident may be given. The bill further requires the Department of General

Services to post and maintain certain information on the agency's website regarding preferences provided by other states.

HB 2158 (Nutter)

Wireless service authority act. Allows multiple localities to create a wireless service authority.

HB 2215 (Albo)

Computer crimes; penalties. Modernizes the Virginia Computer Crimes Act by updating definitions to comport with changing technology, removing superfluous language and relocating language. The bill adds unauthorized installation of software on the computer of another, disruption of another computer's ability to share or transfer information and maliciously obtaining computer information without authority as additional crimes of computer trespass, a Class 1 misdemeanor. The bill also reduces the felony (Class 6) threshold from $2,500 to $1,000 for property damage resulting from computer trespass.

HB 2216 (Albo)

Department of Forensic Science, the Forensic Science Board, and the Scientific Advisory Board created. Creates the Department of Forensic Science as a department within the executive branch of state government and assigns its powers and duties. The bill also creates the Forensic Science Board as a policy board, and the Scientific Advisory Board as an advisory board and likewise assigns their respective powers and duties. The bill also abolishes the Division of Forensic Science within the Department of Criminal Justice Services. The bill contains numerous technical amendments to accomplish this.

HB 2218 (Albo)

Gift certificates; disclosures; penalty. Requires a gift certificate issued by a merchant in Virginia to have permanently affixed to it either an expiration date for the certificate or

electronic card or a telephone number or Internet address at which information about the certificate's expiration and any diminution in value over time may be obtained. A violation of the disclosure requirement is a prohibited practice under the Virginia Consumer Protection Act. This bill is identical to SB 1241.

HB 2273 (Oder)

Remote hunting prohibited; penalty. Prohibits anyone from engaging in computer-assisted remote hunting, or provide or operate a facility that allows a person to engage in such "hunting." Violations are Class 1 misdemeanors and will result in revocation of any hunting license for between three and five years. This bill is identical to SB 1083.

HB 2404 (Philips)

Virginia Freedom of Information Act; exemptions; local wireless service authorities. Excludes from the mandatory disclosure requirements of the Virginia Freedom of Information Act (FOIA) confidential proprietary records and trade secrets developed by or for a local authority created in accordance with the Virginia Wireless Service Authorities Act (§ 15.2-5431.1 et seq.) that provides qualifying communications services as authorized by Article 5.1 (§ 56-484.7:1 et seq.) of Chapter 15 of Title 56 where disclosure of such information would be harmful to the competitive position of the authority. The bill also grants an open meeting exemption for discussions of such records by a local wireless service authority. The bill contains technical amendments.

HB 2470 (May)

Uniform Electronic Transactions Act; local constitutional officers. Includes locally elected constitutional officers in the definition of public body for purposes of the Uniform Electronic Transactions Act.

HB 2471 (May)

Virginia Computer Crimes Act; penalties. Updates the Virginia Computer Crimes Act to include recommendations made by the 2004 joint study on Computer Crimes by the

Joint Commission on Technology and Science and Virginia State Crime Commission. The bill modernizes definitions of "computer", "using a computer" and "without authority" to comport with changing technology. The bill revises provisions regarding computer trespass, a Class 1 misdemeanor, unless the damage to the property of another is $1,000 ($2,500 under current law) or more, in which case it is a Class 6 felony. Provisions regarding computer invasion of privacy are rewritten to include unauthorized gathering of identifying information and Class 6 penalties added for persons with previous convictions, selling or distributing the information to another or using the information in the commission of another crime. The bill adds as a new Class 6 felony using a computer to fraudulently gather identifying information of another (phishing), unless the information is sold or distributed to another or the information is used in the commission of another crime, in which case it is a Class 5 felony. Statute of limitation and venue provisions are relocated in the Code. This bill is identical to SB 1163.

HB 2482 (May)

Personal Information Privacy Act; restricting the use of social security numbers. Prohibits any person from (i) intentionally communicating an individual's social security number to the general public; (ii) printing an individual's social security number on any card required for the individual to access or receive products or services; (iii) requiring an individual to use his social security number to access an Internet website, unless an authentication device is also required; or (iv) mailing a package with the social security number visible from the outside. The bill exempts public bodies and public records. A violation is a prohibited practice under the Virginia Consumer Protection Act. The measure also requires the state employee's health insurance plan to use identification numbers that are not the employee's social security number.

HB 2508 (Welch)

Electronic summons may be used for reportable motor vehicle law violations; citations. Provides that an electronic summons may be used in lieu of a paper summons for reportable motor vehicle violations.

HB 2519 (O'Bannon)

Virginia Immunization Information System (VIIS). Requires the Board of Health, to the extent funds are appropriated by the General Assembly or otherwise made available, to establish the Virginia Immunization Information System, a statewide immunization registry that consolidates patient immunization histories from birth to death into a complete, accurate, and definitive record that may be made available to participating health care providers throughout Virginia. The Board must promulgate regulations addressing voluntary participation, a secure system for data entry or delivery, incorporation of the data already reported on children's immunizations, the nature of the data to be reported, data-sharing agreements with other state and regional immunization registries, use of vital statistic data, requests for records in compliance with existing requirements, release of aggregate data without personal identifiers, and the use of the data in an epidemic or outbreak of a vaccine-preventable disease.

The bill also establishes the criteria for disclosure of protected health information to VIIS, i.e., ensuring the integrity of the health care system and prevention of disease. Immunity is provided to participants, the Board and Commissioner of Health, and employees of the Department of Health. Current responsibilities for record maintenance and obtaining immunization of children are retained as well as existing exemptions on religious or health grounds.

HB 2586 (Cosgrove)

Joint Commission on Technology and Science; clarifications for collegial bodies. Conforms the Joint Commission on Technology and Science's requirements to meet legislative guidelines adopted by the Joint Rules Committee. The bill also makes procedural amendments such as reducing the quorum from six to five members, increasing the term of the chair and vice-chair to a two-year term coincident with the term of office for House members, and changing references from Commission to JCOTS.

HB 2612 (Hugo)

State employees; telecommuting and alternative work schedules. Requires the Secretary of Administration, in developing a telecommuting policy for state employees, to include identification of broad categories of positions determined to be ineligible to participate in telecommuting and the justification for that determination. The bill also requires each agency head in his annual report to the Secretary of Administration to include specific budget requests for information technology, software, or other equipment needed to increase opportunities for telecommuting and participation in alternate work locations.

HB 2631 (Bell)

Computer crimes; penalties. Revises provisions in the Virginia Computer Crimes Act relating to computer fraud and redefines computer invasion of privacy by including the unauthorized gathering of identifying information and punishes subsequent offenses and transferring the information to another or use of the information in the commission of another crime as a Class 6 felony. Currently, the offense is punishable as a Class 1 misdemeanor. Additionally, the fraudulent gathering of such information is punished as a Class 6 felony, a new crime, and transferring the information to another or use of the information in the commission of another crime is a Class 5 felony.

HB 2844 (Saxman)

Competitive Government Act; reporting dates. Changes from January 1, 2006, to October 1, 2005, the date by which the report of the commercial activities being performed by state employees at state agencies and institutions must be completed by the Secretary of Administration. The bill also changes from January 1 to October 1 of each biennium the date by which subsequent reports of examination of commercial activities not already examined must be completed.

HB 2860 (Petersen)

Innovative Technology Authority. Repeals the requirement for the Innovative Technology Authority to establish a technical advisory committee. Other entities now fulfill that role.

HB 2869 (Weatherholtz)

Location and jurisdiction of wiretaps. Redefines jurisdiction for the purposes of electronic or wire interceptions to provide that such communications shall be deemed to be intercepted in the jurisdiction where the order is entered, regardless of the physical location or the method by which the communication is captured or routed to the monitoring location. The bill also provides that an application for an ex parte order authorizing a pen register or trap and trace device may be filed in the jurisdiction where the person or persons who subscribe to the communication system live, work, or maintain an address and that such installation shall be deemed to occur in the jurisdiction where the order is entered, regardless of the physical location or the method by which the information is captured.

HB 2880 (Nixon)

Communications tax reform. Directs the APA to review and collect information in 2005 regarding certain local communications taxes and report to the chairmen of the House and Senate Finance Committees and the Department of Taxation no later than December 1, 2005.

HJ 588 (Marshall, R.G.)

Study; stem cell research. Establishes a joint subcommittee to study medical, ethical, and scientific issues relating to stem cell research conducted in the Commonwealth. The joint subcommittee shall examine the medical, ethical, and scientific policy implications of stem cell research, and the efficacy of research using both adult and embryonic stem cells.

HJ 598 (Parrish)

Study; biodiesel fuel use and production; report. Requests the Secretary of Agriculture and Forestry to study the use and production of biodiesel fuel in Virginia.

HJ 647 (Hamilton)
Commending the Virginia Electronic Commerce Technology on its 10th anniversary.

HJ 689 (Nixon)

Study; cost-effective toll collection. Directs the Joint Commission on Technology and Science to study technologies available for cost-effective toll collection.

HJ 711 (McDonnell)

Resolution; Hydrogen energy. Expresses the General Assembly's support for the Virginia Hydrogen Energy Plan.

HJ 788 (Bryant)

Commending the Central Virginia Governor's School for Science and Technology.

SB 752 (Wampler)

Electronic meetings of the Board of Visitors of the University of Virginia. Extends from 2005 to 2007 the sunset for the exception to the Freedom of Information Act requirements for holding telephonic or video broadcast meetings that has been accorded to the Board of Visitors of the University of Virginia. The bill requires University of Virginia to report to the Virginia Freedom of Information Advisory Council on these meetings, in addition to the Secretary of Education and the General Assembly.

SB 776 (Potts)

Use of the name, logo or symbol of a financial institution; penalty. Prohibits any person from using the name, logo or symbol of a bank, trust company, savings institution, or credit union, or a deceptively similar name, logo or symbol, in any marketing material in a manner that would cause a reasonable person to believe that the material is from the financial institution. A violation is punishable as a Class 1 misdemeanor. In addition, a financial institution whose name, logo or symbol is used in such manner is entitled to injunctive relief, the destruction of the material, and a private action for damages, disgorgement of profit, and attorneys' fees, under the Virginia Trademark and Service Mark Act.

SB 815 (Williams)

"Photo-toll" toll collection programs. Authorizes "photo toll" facilities to record images of all vehicles whose operators choose to use the facilities and bill the registered owners of vehicles as to which no toll is paid, prior to pursuing other remedies. This bill also allows operators to charge an administrative fee of up to $25 when collecting unpaid tolls.

SB 902 (Norment)

Technology Trust Fund Fee. Prohibits, beginning July 1, 2006, transfers from the Technology Trust Fund Fee for purposes not specifically enumerated in the law, including transfers to the general fund.

SB 912 (Norment)

Virginia Consumer Protection Act; fees and costs upon settlement. Provides that if the parties wish to settle a case brought under the Virginia Consumer Protection Act, the court may determine the amount of any award of attorneys' fees or court costs to the plaintiff.

SB 934 (Stosch)

Auditor of Public Accounts; maintenance of database containing historical information. Requires the Auditor of Public Accounts to establish and maintain each year on its Internet web site a searchable database that contains certain state expenditure, revenue, and demographic information for the 10 most recently ended fiscal years of the Commonwealth. The online database shall be made available to citizens of the Commonwealth to allow public access to historical revenue collections and appropriations with related demographic information. The bill also authorizes the Auditor of Public Accounts to perform an audit of the monies furnished to the Washington Metropolitan Transit Authority by the Commonwealth.

SB 959 (Wampler)

Telecommunication and cable television service by localities; release of information. Exempts from the mandatory disclosure requirements of the Freedom of Information Act any public record of a local government that contains confidential proprietary information or trade secrets pertaining to its provision of telecommunication services and cable television service. Public bodies may discuss such records in closed meetings.

SB 963 (O'Brien)

Statewide communications interoperability. Requires the Governor to ensure that the annual review and update of the statewide interoperability strategic plan is accomplished and implemented. The bill also requires all state agencies and localities to achieve consistency with and support the goals of the plan by July 1, 2015, in order to remain eligible to receive state or federal funding for communication programs.

SB 992 (Devolites Davis)

Real Property Electronic Recording Act. Establishes the Real Property Recording Act, which authorizes circuit court clerks to accept and record land records electronically. All

provisions associated with the Act must be reenacted by the General Assembly except for a requirement that the Virginia Information Technology Agency develop standards for electronic recording of land records. A new article in Title 17 restores authority, which had expired July 1, 2004, for court clerks to electronically file other court documents, including instruments and judgments.

SB 1001 (Devolites Davis)

Computer crimes; penalties. Revises provisions in the Virginia Computer Crimes Act relating to theft of computer services, personal trespass by computer, embezzlement, larceny or receiving stolen goods by computer, and civil damages. The bill also relocates statute of limitation and venue provisions in the Code.

SB 1002 (Devolites Davis)

Computer crimes; penalties. Revises provisions in the Virginia Computer Crimes Act relating to computer fraud and redefines computer invasion of privacy by including the unauthorized gathering of identifying information. The bill punishes subsequent offenses and transferring the information to another or using the information in the commission of another crime as a Class 6 felony. Currently, the offense is punishable as a Class 1 misdemeanor. Additionally, the fraudulent gathering of such information is punished as a Class 6 felony, a new crime, and transferring the information to another or use of the information in the commission of another crime is a Class 5 felony.

SB 1027 (Newman)

Virginia Information Technologies Agency; Virginia Information Providers Network. Dissolves the Virginia Information Providers Network as a separate division of the Virginia Information Technologies Agency (VITA) and gives its authority directly to VITA.

SB 1083 (Ticer)

Remote hunting prohibited; penalty. Prohibits anyone from engaging in computer-assisted remote hunting, or provide or operate a facility that allows a person to engage

in such "hunting." Violations are Class 1 misdemeanors and will result in revocation of any hunting license for between three and five years. This bill is identical to HB 2273.

SB 1132 (Howell)

Virginia Immunization Information System (VIIS). Requires the Board of Health, to the extent funds are appropriated by the General Assembly or otherwise made available, to establish the Virginia Immunization Information System, a statewide immunization registry that consolidates patient immunization histories from birth to death into a complete, accurate, and definitive record that may be made available to participating health care providers throughout Virginia. The Board must promulgate regulations addressing voluntary participation, a secure system for data entry or delivery, incorporation of the data already reported on children's immunizations, the nature of the data to be reported, data-sharing agreements with other state and regional immunization registries, use of vital statistic data, requests for records in compliance with existing requirements, release of aggregate data without personal identifiers, and the use of the data in an epidemic or outbreak of a vaccine-preventable disease.

The bill also establishes the criteria for disclosure of protected health information to VIIS, i.e., ensuring the integrity of the health care system and prevention of disease. Immunity is provided to participants, the Board and Commissioner of Health, and employees of the Department of Health. Current responsibilities for record maintenance and obtaining immunization of children are retained as well as existing exemptions on religious or health grounds. This bill is identical to HB 2519.

SB 1147 (Obenshain)

Computer crimes; phishing; penalty. Makes it a Class 6 felony to fraudulently obtain, record, or access from a computer the following identifying information of another: (i) social security number; (ii) driver's license number; (iii) bank account numbers; (iv) credit or debit card numbers; (v) personal identification numbers (PIN); (vi) electronic identification codes; (vii) automated or electronic signatures; (viii) biometric data; (ix)

fingerprints; (x) passwords; or (xi) any other numbers or information that can be used to access a person's financial resources, obtain identification, act as identification, or obtain goods or services. Any person who sells or distributes such information or uses it to commit another crime is guilty of a Class 5 felony.

SB 1148 (Stolle)

Virginia Research and Technology Advisory Commission. Increases the membership of the Virginia Research and Technology Advisory Commission from 29 to 31 by adding the Eastern Virginia Medical School as an academic research institution member and by adding an additional member representing research- and technology-intensive industries appointed by the Governor. The bill also includes technical amendments to reference the correct titles and names of certain ex officio members and to alphabetize the research institutions. This bill is similar to HB 1691.

SB 1159 (Stolle)

Wireless E-911 Services Board. Clarifies that the Wireless E-911 Services Board's obligation to make payments to PSAP operators and CMRS providers is subject to the extent of appropriated funds. The bill also removes the exemptions to E-911 deployment, excludes governments from the surcharge collection, and establishes July 1 as the deadline for late funding requests. In addition, the bill clarifies the appeals process and expands the Board's responsibilities to include development of a single, statewide electronic addressing database.

SB 1163 (Stolle)

Computer crimes; penalties. Modernizes the Virginia Computer Crimes Act by revising definitions of "computer", "using a computer" and "without authority." The bill revises provisions relating to computer trespass and reduces thresholds for damages. Gathering identifying information (phishing) is punished as a felony. Statute of limitation and venue provisions are relocated in the Code. This bill is identical to HB 2471.

SB 1192 (Devolites Davis)

Posting and availability of certain information on the Internet. Clarifies that circuit court clerks may provide secure remote access to any document that is filed among the land records in the circuit court, and also allows the clerks to provide secure remote access by any person and his counsel to documents filed in matters to which such person is a party. "Land records" are defined as those records authorized to be recorded that affect title to real property. Nothing in the revised statute prohibits the Supreme Court or other courts from providing online access to a case management system that may include abstracts of case filings and proceedings in the courts of the Commonwealth. The sunset clause applicable to this section is extended from July 1, 2005, to July 1, 2007.

SB 1194 (Potts)

Christopher Reeve Stem Cell Research Fund. Establishes a special nonreverting, revolving and permanent fund for the support of stem cell research in honor of Christopher Reeve. The Fund will be used to support medical and biomedical stem cell research conducted in Virginia institutions of higher education relating to the causes and cures of disease, including, but not limited to, paralysis caused by spinal cord injury, diabetes, cancer, heart disease, and neurological disorders, such as Lou Gehrig's disease. No moneys from the Fund may be provided to any entity that conducts human stem cell research from stem cells obtained from human embryos, or for conducting such research; however, research conducted using stem cells other than embryonic stem cells may be funded. The Fund will consist of appropriations, gifts, grants, and donations from public or private sources, will be administered by the Commonwealth Health Research Board (an existing board with appropriate expertise), will not require matching funds from the institutions, and may be used to support stem cell research that is not eligible for federal research funds through the National Institutes of Health.

SB 1196 (Newman)

Freedom of Information Act; electronic communication meetings. Reduces the notice required for electronic communication meetings from 30 days to seven working days. The bill also (i) eliminates the 25 percent limitation on the number of electronic meetings held annually; (ii) eliminates the requirement that an audio or audio/visual recording be made of the electronic communication meeting, but retains the requirement that minutes be taken pursuant to § 2.2-3707; (iii) allows for the conduct of closed meetings during electronic meetings; (iv) changes the annual reporting requirement from the Virginia Information Technology Agency to the Virginia Freedom of Information Advisory Council and the Joint Commission on Technology and Science; and (v) expands the type of information required to be reported. The bill specifies that regular, special, or reconvened sessions of the General Assembly held pursuant Article IV, Section 6 of the Constitution of Virginia are not meetings for purposes of the electronic communication meeting provisions. The bill also defines "electronic communication means." The bill is a recommendation of the VA Freedom of Information Advisory Council and the Joint Commission on Technology and Science. This bill incorporates SB 711.

SB 1241 (Devolites Davis)

Gift certificates; disclosures; penalty. Requires a gift certificate issued by a merchant in Virginia to have permanently affixed to it either an expiration date for the certificate or electronic card or a telephone number or Internet address at which information about the certificate's expiration and any diminution in value over time may be obtained. A violation of the disclosure requirement is a prohibited practice under the Virginia Consumer Protection Act. This bill is identical to HB 2218.

SJ 406 (Rerras)

Hydrogen energy. Expresses the General Assembly's support for the Virginia Hydrogen Energy Plan.

SJ 412 (Martin)

Confirming Governor's appointments; certain Secretaries, agency heads, and personnel. Confirms interim appointments made by Governor Warner of the Secretaries of Agriculture and Forestry and of Technology, certain agency heads, and personnel.

SJ 414 (Martin)

Confirming Governor's appointments; commerce and trade. Confirms interim appointments made by Governor Warner related to commerce and trade.

SJ 420 (Martin)

Confirming Governor's appointments; technology. Confirms interim appointments made by Governor Warner related to technology.

SJ 422 (Martin)

Confirming Governor's appointments; miscellaneous positions. Confirms interim appointments made by Governor Warner to certain compact agencies, designated agencies, independent agencies, and miscellaneous positions.