Wednesday, September 8, 2004, 9:30 a.m.
House Room D
General Assembly Building
Richmond, Virginia

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 from those wanting to do harm, 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, FBI, discussed the FBI's national initiative to provide forensic analysis and assist state and local law enforcement, as well as an overview what they can recover 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 told JCOTS that it is a unique law enforcement partnership that promotes quality and strengthens computer forensics laboratory capacity. For the communities that they serve, RCFLs conduct forensic exams on all types of digital evidence, assist on searches, and train law enforcement. While they do not conduct investigations, the RCFL examiner provides 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 such 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 with approximately $1 million in annual operating costs. 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, investigators lock a suspect's hard drive and retrieve active graphics files for use in prosecutions. He explained that they retrieve these files even if the suspect has deleted them. When someone deletes a file in a Windows system, all he really does is change the first character of the file name in the File Allocation Table (FAT) to the lower case Greek letter sigma. 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.

Not only can they retrieve documents that have been deleted, but they can also retrieve documents when the system has been damaged. In one case, when the FBI knocked on the door of a suspected child pornographer and announced that they were executing a search warrant, the subject dropped his laptop computer into the bathtub. Examiners recovered the laptop, drained the water, and recovered all data from the hard drive. In another case, during the FBI's investigation of a child predator, "traveler" case, 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, Agent Kacoyannakis pointed out that not all data can be recovered. Most notably, one that got away used a 12-gauge shotgun to permanently destroy the hard drive so that investigators could not recover any data.

He cautioned the members that not all searches are announced. Hackers, as they get more sophisticated, can steal any information stored on unsecured system without anyone's knowledge. Some of them can even hack into a secure system and steal information.

Computer Forensics in Virginia

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

Sergeant Keeton explained that CERU, like the RCFL, performs forensics exams and testify, but unlike the RCFL, CERU examiners also analyze the information. 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, mostly local. A CERU only costs approximately $50,000 to start and $20,000 - $30,000 for annual training.

After Sergeant Keeton's introduction, Ms. Bryce reviewed the computer crimes laws in Virginia and the types of evidence hidden in various devices. She reminded JCOTS that any digital or

electronic device which 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 or 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 to systems and vulnerabilities (i.e., exposures of systems). It should include all resources - people, technology, and operations. Everyone in the organization must support and adhere to the security policy. The organization should limit access to information based on job functions and a 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. They include up-to-date virus protection software, firewall systems technology, intrusion detection, encryption, and network devices (i.e., routers, switches, etc.). All of this technology, if properly used and regularly updated, can limit exposure to malicious software and intruders.

Operational resources begin 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. Regardless of where it comes from, 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 discovered by accident and employees usually discover them. However, they need to know what to report and to whom for organizations to utilize them effectively. 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; they control the lifeblood of the organization.

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 (Additional duties of the CIO relating to security of government database) 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 to VITA four tasks for developing a statewide information technology security plan. VITA must 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.

Mr. Deason cautioned JCOTS that the risks from these threats are real. 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 is the same: the possible loss of confidential information, interruption of critical systems, or even potential legal violation and liability.

VITA's security planning follows two basic principles. First, the Commonwealth must protect the confidentiality, integrity, and availability of information systems. Second it should treat security as a critical enabler, but it must be done right and it must be built in to a system, not an afterthought. As we build more enterprise systems and work with more partners, the Commonwealth has both an opportunity to develop a statewide security system and a risk with increased exposure to systems over which it has no control. Because security is so critical, VITA will rely on no one solution

By mid-April 2005, VITA plans to complete an enterprise security risk assessment. By the end of the first half of 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 are currently available to 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 face recognition, fingerprint, hand geometry, iris, palm prints, signature and voice. Biometric technologies can work in two modes – authentication (one-to-one matching) and identification (one-to-many) matching. However, only three biometrics are capable of the latter – face, finger and iris.

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 his 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 where an intruder could access them. When a finger 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 which is discarded after feature extraction. Since the template only holds information about points located on your fingerprint, the original image cannot be restored.

While this technology is not foolproof, it is most common for providing basic security such as entry to homes and non-critical computers and information. In addition, altered fingerprints, such as burning them off or severely cutting fingers, can affect the system's ability to match them, as can changes in skin elasticity caused by age.