

Department of Information Technology

70-05-Information Security and Protection

Fund/Agency: 001/70		Department of Information Technology	
Personnel Services	\$323,970	<p>CAPS Percentage of Agency Total</p> <p>0.8%</p> <p>99.2%</p> <p>■ Information Security and Protection ■ All Other Agency CAPS</p>	
Operating Expenses	\$0		
Recovered Costs	\$0		
Capital Equipment	\$0		
Total CAPS Cost:	\$323,970		
Federal Revenue	\$0		
State Revenue	\$0		
User Fee Revenue	\$0		
Other Revenue	\$0		
Total Revenue:	\$0		
Net CAPS Cost:	\$323,970		
Positions/SYE involved in the delivery of this CAPS	5/5		

► CAPS Summary

The Information Security and Protection CAPS in the Department of Information Technology (DIT) is responsible for ensuring the implementation of information security practices within the County government that gain public confidence and protect government services, privacy and sensitive information. The role of Information Security Management is to protect the confidentiality, integrity, and availability of systems, networks, and data. In order to institute this management framework for information security, the information protection staff continually serve as (1) catalysts for ensuring that information security risks are considered in both planned and ongoing operations, (2) central resources for advice and expertise to units throughout the organization, and (3) a conduit for keeping top management informed about security-related issues and activities affecting the organization.

Department of Information Technology

Specific activities of the Information Security Management staff include:

- exploring and assessing information security risks to business operations;
- researching potential threats, vulnerabilities, and control techniques and communicating this information to others in the organization;
- determining what policies, standards, and controls are worth implementing to reduce these risks;
- developing and adjusting countywide policies and procedures to ensure information systems reliability and accessibility, and to prevent and defend against unauthorized access to systems, networks and data;
- promoting awareness and understanding of security issues among program managers, computer users, and systems development staff and ensuring sound security principles are reflected in organization's visions and goals;
- developing and implementing programs to ensure that systems, network, and data users are aware of, understand, and adhere to systems security policies and procedures;
- participating in assurance of security compliance with regulatory requirements;
- participating in network and systems design to ensure implementation of appropriate systems security policies;
- conducting risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs;
- developing systems security contingency plans and disaster recovery procedures;
- monitoring various aspects of the organization's security-related activities;
- establishing a computer incident response capability, and, in some cases, serving as members of the emergency response team;
- accounting for the number and types of security incidents;
- facilitating the gathering, analysis, and preservation of evidence used in the prosecution of computer crimes;
- assessing security events to determine impact and implementing corrective actions;
- ensuring the rigorous application of information security/information assurance policies, principles, and practices in the delivery of all Information Technology services.

The concept of Information Protection was initially introduced into Fairfax County in approximately 1982 with the establishment of an Computer Security Group. At that time, efforts were strictly limited to defining users and providing access control to applications located on a IBM mainframe Computer. Since that time, automated information processing has become more de-centralized and resulted in the creation of an enterprise network, and, in some cases, agency-specific networks that are integrated into the County's Enterprise Network. Additionally new technologies, such as the Internet and Intranet, were employed which precipitated a need for a new Information Security Architecture and Infrastructure support. Security objectives turned outward from internal User ID and password administration and

Department of Information Technology

mainframe access control, to decentralized management. To facilitate this decentralized approach, Agency Information Protection Coordinators (AIPCs) were appointed within agencies to coordinate information protection issues with DIT's information protection staff. The duties of the AIPCs were expanded from User ID and access control administration to include security education, awareness and training. This new role was documented in the Fairfax County Information Protection Manual (IPM) that was initially published in May 1999. The IPM provides the framework for the new Security Infrastructure. As a result of this movement, the Information Security program currently consists of centralized management with decentralized activities. However, program oversight rests with the Information Protection Officer within DIT who is responsible for establishing standards, monitoring activities and establishing protection criteria.

Initiatives

A number of significant initiatives occurred during FY 2001 to extend and enhance the capabilities and services provided by Information Security Management.

- **Use of Consulting Services.** As the County migrated from a single computer platform to a more distributed information-processing environment over an enterprise network, it became evident that security-consulting services were needed. Specifically as we began to develop our e-government initiatives, it became imperative that several parallel actions were required.

Approximately three years ago, consulting services were used to perform an evaluation of our existing firewall topology and rule set. Results of this effort included findings that caused a change in firewall topography and ultimately employment of a new firewall technology.

Approximately two years ago, a consulting firm was employed to perform a countywide vulnerability assessment to determine our security posture in regard to our vulnerability to malicious hacking. A phased approach was employed and this activity is continuing to date. Initial findings have resulted in improvements to the network perimeter. Additionally, general information security support Statements of Work have been issued and support has been provided in policy development, analysis and the providing of security recommendations. Use of consultants has already proved invaluable and a stronger information protection posture is currently in place.

- **Perimeter Vulnerability Assessment.** The objective of performing the network perimeter vulnerability assessment has been to establish the County of Fairfax's security baseline as it relates to electronic threats and vulnerabilities associated with Internet connectivity. Through contractual support, commercial and public domain tools often employed by hackers, were used to perform analysis on Fairfax County devices that are Internet-accessible. The information that is acquired from the scan identifies potential weak points in configuration and/or architecture. The findings provided the impetus for the implementation of processes and procedures required to minimize risk and improve the County's security posture.
- **War-Dialing Assessment.** The objective of performing the War-Dial has been to attempt to establish a connection to remote access servers or unregistered modems behind the perimeter or firewall, as well as searching for weak security points, such as common usernames and weak passwords. Through contractual support, extensive scanning has been performed on a sample block of analog phone numbers. The information provided from this scan is being utilized to eliminate unsecured remote access.

Department of Information Technology

- **Internal Network Scanning Assessment.** Internal scanning detects unauthorized capabilities on the internal network. Through contractual support, commercial and public domain tools were used to perform the analysis. The results of this analysis are being utilized to address vulnerabilities associated with system configuration, unidentified or undocumented services and equipment, and to address network segmentation issues.
- **Network Architecture Review.** The objective of performing the network architecture review has been to evaluate the current and planned network architecture and recommend enhancements to increase the security of the proposed network.
- **Firewall Ruleset Analysis.** The objectives of performing a ruleset review have been to evaluate the firewall ruleset and provide configuration guidance for the proper secure configuration of the firewall. This analysis has led to development of a draft firewall policy and documented process and procedures for making changes to the firewall.
- **Digital Signatures.** In December 1999, the County joined the Commonwealth of Virginia in accomplishing a proof-of-concept for the use of Digital Signatures within Virginia. Fairfax County participated in a pilot program with the Department of Motor Vehicles in Richmond, VA, to electronically transmit and receive revenue-generating reports. Reports were electronically generated in Richmond, digitally signed and transmitted using e-mail to the Department of Tax Administration (DTA) in Fairfax County. Within the DTA, the reports were analyzed, validated, and verified. The final report was signed with a digital signature and then transmitted via e-mail back to DMV. This pilot was a success and proved that digital signatures could be used within our technical infrastructure environment.

Fairfax County continues to work with the Digital Signature Implementation effort with the Commonwealth. Fairfax County is the representative for local governments on the state Commercial Off the Shelf Software (COTS) Digital Signature Implementation subcommittee.

Currently, efforts are being undertaken to work with County agencies to identify documents that are being sent to Richmond to determine if these documents could be sent in an electronic format with an electronic/digital signature. Additionally, other internal County documents are being evaluated to determine the feasibility of using electronic documents with electronic/digital signatures. A digital signature process will be in place and operational during this fiscal year.

- **E-government Security.** The Security Infrastructure is evolving to meet the increased need for e-government activities. Initial efforts are underway to identify, evaluate, and implement software and hardware products and e-commerce methodologies, to make the security architecture more robust to adequately handle e-government challenges. Specific efforts have been directed towards Public Encryption Infrastructure (PKI) capabilities. The first PKI efforts were employed approximately two years ago with the use of digital certificates at the server level. Certificates, which identified specific Internet servers and provided encryption capabilities, were installed and used on Internet Servers to enable encrypted server-to-server communications.

Department of Information Technology

Accomplishments

- **Anti-Virus Protection.** The County uses the Three-Tier protection model with anti-virus software employed at the Internet Gateway, on servers and on desktop/laptops. With the implementation of a new firewall, anti-virus software will be employed at the firewall level. Approximately one year ago, an intensive effort was undertaken to identify all servers and desktop/laptops and ensure that virus protection software was employed and current. Since that time education efforts, along with procedures, have been developed and implemented to ensure that all users keep anti-virus software current. In addition, virus protection was expanded on the Outlook E-mail platform by employing anti-virus software with the capability to perform subject-line filtering. Currently the majority of malicious code attacks (e.g. virus, Denial of Service, WORM, etc.) are being stopped preventing an infection of the system.
- **Firewall Implementation.** External communications entering the County's system are routed through dedicated circuits or via the Internet. All external traffic transiting the Internet is routed through a firewall before access to the County's system is granted. Behind the firewall the County has implemented a public/private network topology. Platforms that contain publicly accessible information are located on the public network. Platforms that require more protection are located throughout the private side. The firewall is implementing controls to ensure that the majority of external hosts are denied access to the internal network.
- **Mainframe to Decentralized Network Infrastructure.** The Security Infrastructure currently in effect is a centrally managed enterprise effort using decentralized computing platforms. Every County user is granted the required access necessary to perform job functions. User identification and authentication is based upon a unique User ID that is used to create access accounts on the mainframe, network, servers, and other platforms. Auditing on all platforms is conducted based upon this User ID. Users are authenticated to the system by using passwords uniquely connected to the User ID. Security functionality (i.e. User Identification and Authentication, Access Control and Auditing) is accomplished at the operating system, with such functionality that is inherent to the operating system, and at the application level using internal access tables and application specific controls.
- **Use of Security Tokens for Dial-Up Remote Access.** Within the County, Dial-Up Remote access is granted to individuals who are approved telecommuters; users who periodically need to access the system from home or other locations, and individuals who need access while traveling. By use of Dial-Up Remote access the user is provided the same access as if the user were physically present at his or her workstation. Within the past two years, the Dial-Up Remote access program received a major upgrade. Dial-Up Remote authentication moved from a call-back authentication procedure to use of security tokens, which provide two-factor authentication. An authentication server was added to the network and is used to identify and authenticate users. Each user is issued a security token that is used in conjunction with the user's unique identifier to provide the two-factor authentication.

Department of Information Technology

► Method of Service Provision

Services are provided primarily by internal staff. Consultants/contractors are utilized as needed for special projects or for areas where additional staffing is needed.

► Performance/Workload Related Data

Title	FY 1998 Actual	FY 1999 Actual	FY 2000 Actual	FY 2001 Estimate	FY 2002 Estimate
User Accounts Supported	N/A	23,897	25,402	27,588	28,800
Dial-Up Remote Access Accounts Supported	N/A	642	860	1,350	1,500
Security Administrative Support Actions	N/A	21,592	14,500	13,800	11,000