Response to Questions on the FY 2005 Advertised Budget Plan

Request By: Supervisor Gross

Question: Of the $1.3 million budgeted in Fund 104, Information Technology for Enhanced County Security, how much is included to address computer viruses? Also, what has it cost the County over the last two years to address viruses?

Response: The $1.3 million budgeted in Fund 104, Information Technology supports security technology to address several types of malicious activity which include viruses, hackers and denial of service attacks that could disable County systems or destroy County data. The funding includes $326,000 for on-line authentication of the identity of persons requesting access to County systems and data. This is especially important to the continued implementation of e-government services in addressing privacy concerns of the public. This would enable persons to establish identifiers other than use of social security numbers. This type of technology will soon become a national standard for interactive services. Funding of $400,000 is for security monitoring tools as required by County audit recommendations, and for Health Insurance Portability and Accountability Act (HIPAA) audit requirements. Further, it will reduce manual audit tasks associated with the growing number of forensics investigations performed by DIT staff and it will expedite audit investigations and will flag potential violations for earlier intervention. The remaining $534,667 will improve the functionality of and support an expansion of the County's firewall, to further prevent unauthorized access to the County's network. This includes attempts to introduce new viruses to the network from the Internet and from other communications, such as e-mail.

The FY 2005 investment will augment the current virus management and intrusion detection program implemented as part of the overall security system over the past three years. As widely reported in the media, there has been exponential growth in viruses and malicious activity; which if not controlled, could negatively impact County staff efforts to protect information resources, and the services and support provided to County residents.

The County's current architecture consists of eight firewalls that are set up around County systems. In FY 2003, there were approximately 4.2 billion attempts to interact with the County from outside the firewalls. Of these potential transactions, 1.6 million or 38 percent were blocked as potential viruses or security breach attempts. This number is expected to continue to increase, pointing to the importance of vigilant information security. It should also be noted that there were 9.5 million visits to the County's website last year that also had to be monitored for potential security breach attempts.

To combat this growing problem, the Department of Information Technology has purchased hardware and software associated with virus management, and has provided contractor and County personnel support to both investigate and resolve virus incidents as well as proactively implement additional anti-virus support. The following table reflects FY 2003 actual and FY 2004 year-to-date spending on these activities.

	FY 2003 Actual	**FY 2004 Year-to-Date**	**Total**
Hardware and Software	$334,400	$429,400	$763,800
Personnel and Contract Support for Resolving Incidents	$747,500	$1,347,500	$2,095,000
Personnel and Contract Support for Proactive Measures	-	$214,500	$214,500
Total	$1,081,900	$1,991,400	$3,073,300

The activities above, and necessary funding to support them, have increased significantly in the last year requiring much of the funding to be absorbed from DIT infrastructure budgets. This has deferred baseline maintenance requirements, increasing the potential of agency business disruptions due to failures and slowing DIT's ability to respond to normal IT service requests.