County of Sacramento
Inter-Departmental Correspondence

For the Agenda of: June 2, 2005

Date: May 17, 2005

To: Information Technology Policy Board Members

From: Debbie Nadolna, Chair
Technology Review Group

Subject: Approve the Recommendation for Encryption Policy and Standards

Recommendation:

- Approve the Encryption Policy
- Approve the Encryption Standards described in Attachment A

Scope:

This policy provides direction to ensure that the County of Sacramento has done its due diligence to protect data from unauthorized access.

Background:

The County of Sacramento Information Technology Plan for 2005, Focus Area 1, Goal 6, Objective A states the following:

Develop encryption standards for electronic communications outside the County.

A team of individuals from the District Attorney MIS, Department of Human Assistance MIS, Employment Services Risk Management MIS, Municipal Services Agency MIS, OCIT and Voter MIS was formed to develop the policy and standard. The team determined the scope of the assignment and conducted research to determine what should be included in the policy as well as when it should be implemented.

Discussion:

As the County continues with the implementation of E-Government and connecting to non-county organizations and individuals, it is becoming more important to protect certain types of data. Also, new federal regulations governing the Health Insurance Portability and Accountability Act (HIPAA) require the implementation of technical policies and procedures for electronic information systems that maintain electronic protected health information and to allow access only to those persons or software programs that have been granted access rights.

The Electronic Data Access Policy dated August 20, 2000, and approved by the Information Technology Policy Board on October 5, 2000, provides for the data classifications of non-sensitive, sensitive, and confidential. As indicated in this policy, it is the responsibility of the department head to determine the classification of the data they own.

In addition to data classification, a risk assessment needs to take place to determine what damage will be done from unauthorized access. Once the data classification and risk level has been established then a decision can be made on whether to encrypt the data.

Encryption is a tool that can be used to ensure that data is protected from unauthorized access. There are two “states” that data can exist. Data can be “at rest” or stored, or it can be “in transit” or traveling across the network to its destination to be processed or viewed.

Encryption has its limits and should only be used when appropriate. Non-sensitive data does not need to be encrypted. Sensitive and confidential data may need to be encrypted depending upon an analysis on how the data is stored (at rest), how it is used and how it gets to where it will be used (in transit).

Policy Statement:

Encryption of data deemed sensitive or confidential is required when legally mandated, or if the risk of unauthorized access would require encryption. It is the responsibility of the owner of the data to perform a risk assessment of the data they own. Proven, standard algorithms should be used as the basis for encryption technologies. The use of proprietary encryption algorithms is not allowed for any purpose unless authorized by the Chief Information Security Officer.

Please refer to the Attachments for definitions, guidelines and technical standards for encryption.

Impact of Implementing the Policy:

Encryption of protected data could potentially cause technical issues with performance and management of the County’s IT infrastructure and IT Systems. It may require changes to the infrastructure to implement. Staff awareness is critical and training may be required.

Attachment A

Encryption Standards

The County of Sacramento Encryption Policy governs when encryption must be used to protect County protected information. This standard identifies acceptable encryption technologies for protecting confidential information when encryption is required.

I. Scope

These standards apply when encryption is required of information owned or managed by the County of Sacramento.

II. Supported Encryption Technologies

This section identifies approved encryption algorithms and protocols for meeting encryption requirements for information as specified in the County of Sacramento Encryption Policy.

Security professionals and industry analysts consider the algorithms in the attached standards to be strong when used with adequate key sizes. While it is theoretically possible to decrypt information encrypted with these algorithms, the amount of time and computing power required to do so is sufficiently large thus mitigating the risk of compromise to an acceptable level.

The algorithms and protocols are approved by industry standards organizations including the National Institute of Standards and Technology (NIST) and are readily available in vendor products. Use of the approved algorithms and protocols will facilitate interchange of encrypted information between the County and business partners.

The intent of these standards is to:

- Require strong encryption to prevent compromise of confidential information if it is accessed by someone without proper authorization.
- Specify use of industry standard protocols to facilitate exchange of information between business partners and customers who have a right to access the information.

<u>The following encryption algorithms and protocols are approved under this standard:</u>

*Symmetric key encryption algorithms***:**

- Advanced Encryption Standard (*AES*) – the symmetric encryption algorithm of choice.
- Triple Data Encryption Standard (Triple DES).
- DES – grandfathered for legacy systems only. Recommend upgrade to AES or Triple DES.

The minimum key size acceptable for new deployments of symmetric key encryption is 128 bits. When DES is grandfathered for legacy systems, 64 bit keys are permitted.

Asymmetric key (Public key) encryption algorithms:

- Digital Signature Standard (DSS).
- Rivest, Shamir, and Adelman (RSA).
- Elliptic Curve Digital Signature Algorithm (ECDSA).

Recommended Encryption protocols:

- IPSec VPN.
- Secure Sockets Layer Version 3 (SSLv3) – This includes SSL VPNs.
- Transport Layer Security Version 1 (TLSv1).
- Secure Shell Protocol (SSH). New applications secured using SSH should use SSHv2.
- Secure Multipurpose Internet Mail Extensions (S/MIME).

Legacy Encryption protocols:

- Point-to-Point Tunneling Protocol (PPTP) VPN – grandfathered for legacy systems only. Recommend upgrade to IPSec or SSL VPN.
- Layer 2 Tunneling Protocol (L2TP) VPN – grandfathered for legacy systems only. Recommend upgrade to IPSec or SSL VPN.
- SSHv1 is grandfathered for legacy systems only.

Key exchange:

These standards do not require specific protocols or methods for key exchange, but they do require the department to implement procedures for secure exchange and management of encryption keys for applications/information systems that implement encryption.

Standards for Information in Transit

Departments can encrypt information transmitted over a network at several different points (layers) as it is prepared for transmission. These include:

1. The applications that sends and receive the information
2. The communication link (session) established between computers that send and receive the information
3. The network hardware/software that packages the information for transmission across the physical network media (the wire, optical fiber, etc.).

These standards specify approved algorithms and protocols for encrypting information at different levels. It is **not** necessary to encrypt information at more than one level. For example:

- If information is being transmitted over a Virtual Private Network (VPN) where all network traffic is encrypted, departments do not need to deploy encryption at the session or application level.
- If information is transmitted between nodes on the County's Wide Area Network (WAN) and network level encryption is deployed between those nodes, departments do not need additional encryption between those nodes.

  These standards do not dictate the level of encryption departments should apply. Departments should choose the level based on cost and the business requirements for deploying the information system.

Application of the standard for encrypting e-mail

Several of the approved encryption protocols can be used to encrypt e-mail. The preferred method for e-mail encryption will depend on the department's business requirements, including the location and number of people that need to send and receive confidential information.

With *end-to-end encryption using S/MIME*, the user's e-mail client encrypts and decrypts the e-mail. Each user must have a digital certificate and e-mail is encrypted throughout its transmission regardless of the path taken over the Internet, County WAN, and department Local Area Networks (LAN's). This method works well for small groups where it is feasible for users to manage certificates for people they communicate with. For large groups, a public key infrastructure would need to be implemented to support certificate/key management.

Alternatively, a department can use *gateway-to-gateway encryption using S/MIME*. This approach uses similar technology as end-to-end encryption but performs the encryption and decryption at a server rather than at a users e-mail client. Rather than assign each user a digital certificate, the keys are assigned at an organizational level. With this option, e-mail is encrypted as it is transmitted between the e-mail server of the sending and receiving organization. This option does not encrypt e-mail on the departments LAN nor does it provide for e-mail encryption when accessed from a remote site or portable device. Use must be coordinated with OCIT Exchange Email Services Team.

For distribution of confidential information to a single person or small group, it is also acceptable for the department to transmit encrypted files using any of the approved algorithms via e-mail. When departments use this approach, they must implement procedures to ensure encryption keys are distributed and managed in a secure manner.

When departments permit e-mail access via the Internet or from a portable device and encryption is required, the e-mail must be encrypted when it is transmitted to the web client or portable device. Any of the approved algorithms or protocols can be used to support remote e-mail access.

Application of the standard to applications transmitting confidential information

The preferred method for encrypting confidential information transmitted by an application will depend on the requirements for the application. SSLv3 (or TLSv1) is supported by web browsers and does not require additional client software. It can encrypt information transmitted between the user's workstation (or other device) and the application server regardless of the path the information takes over the network(s).

Encrypted tunnel VPN's may provide a higher level of security (due to frequent re-negotiation of encryption keys) but require installation of the VPN client software at the user location.

Application of the standard to file transfer

The preferred method for transfer of files containing confidential information is to transmit the files over an encrypted VPN (PPTP, L2TP, IPSec) or encrypted session (SSH, SSLv3, or TLSv1).

Department can also encrypt files using one of the approved symmetric key encryption algorithms and transmit them via e-mail. This alternative requires secure communication of the encryption key, and department should only use this method for infrequent file transfers and small files.

Encryption of information transmitted for printing

Department can encrypt print streams directed to a printer and transmitted over the Internet or the County WAN using an encrypted session or VPN tunnel (PPTP, L2TP, IPSec, SSLv3, or TLSv1). For mainframe applications, the preferred method is to establish an encrypted session using Host On Demand (HOD).

For applications printing on the County's WAN, network level encryption meets the requirement of this standard.

Acceptable methods for encrypting wireless LAN's

Please refer to the TRG approved Wireless Data Networking Policy and Standards dated December 4, 2003. The document can be found at http://www.itpb.saccounty.net.

Encryption for remote access with mobile devices

When remote access to a department LAN is supported and encryption is required, the department must encrypt information when transmitted between the remote site or mobile device and the department network. There is no preferred method for encrypting remote access transmissions, but departments must use one of the approved algorithms/protocols. The preferred method will depend on the algorithms/protocols supported by the mobile device and remote access a department deploys.

Standards for Stored Information

Application of the standard for encrypting passwords

Departments must evaluate products used to manage information under their control to ensure strong password encryption is used.

Application of the standard for encrypting information stored on laptop PC's or other mobile devices

The approved methods of encryption for use on laptop PC's and other portable storage devices are file level and full disk encryption. The preferred method for encryption on laptop PC's and other portable storage devices is full disk encryption. With full disk encryption, everything on the hard disk, including the operating system as well as the applications and data files are encrypted. Full disk encryption does not rely on users to decide what files need to be encrypted.

File level encryption is approved on laptop PC's when the sensitivity of data does not warrant the use of full disk encryption. The use of File level Encryption is also acceptable on data of a more sensitive nature as long as the data is not unencrypted or manipulated while stored on the laptop PC. In this case the laptop or storage device is serving as a transport for encrypted data. Any encryption product that uses algorithms from the list of approved algorithms (above) is acceptable. The implementation and use of this technology is left to individual departments to fit its business and security needs.

Application of the standard for encrypting information stored on a server

Departments may use *file level encryption* to protect only those files that require encryption. Any file encryption product using algorithms from the list of approved algorithms (above) is acceptable.

It is important that departments implement recovery agent(s) as a safeguard to decrypt data that was encrypted by another user. Recovery agents are useful, for example, when employees leave the company and their remaining data needs to be decrypted. The recovery agent has a special certificate and associated private key that allow data recovery for the scope of influence of the recovery policy implemented by the department. The recovery agent can be scoped for a single local server or for domain wide authority. The implementation is left to departments to fit business and security needs.

Application of the standard for encrypting information stored on portable media

Products that encrypt all information copied to a portable media are preferred. Alternatively, agencies may use products that encrypt only selected files. Any encryption product using algorithms from the list of approved algorithms (above) is acceptable.

Attachment B

The following risk assessment process was developed by the team that implemented the HIPAA Security Rule in Sacramento County. Owners of data can use this process (or develop their own) to identify the risk of unauthorized access to protected data. Use the following link to access the document.

Gap Analysis and Risk Assessment

Attachment C

DEFINITIONS

Advanced Encryption Standard – The Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and is likely to become the de facto encryption standard for commercial transactions in the private sector. (Encryption for the US military and other classified communications is handled by separate, secret algorithms.) AES was selected by the National Institute of Standards and Technology as a more robust replacement for the Data Encryption Standard (DES) and to a lesser degree Triple DES. AES uses a symmetric algorithm (same key for encryption and decryption) supporting key sizes of 128, 192 and 256 bits.

AES – See Advanced Encryption Standard

Asymmetric Key Encryption – Asymmetric key encryption is also known as public key encryption. It uses different keys to encrypt and decrypt a message. Under this system everyone gets a pair of keys: a public key which is published for all to see and use, and a private key which is to be kept secret. The public key could then be used to encrypt a message, which only the holder of the private key, could decrypt and read.

Data Encryption Standard – Data Encryption Standard (DES) is a widely used method of data encryption using a private (secret) key technology. DES applies a 56-bit key to each 64-bit block of data. Early in 1997, Rivest-Shamir-Adleman, owners of another encryption approach, offered a $10,000 reward for breaking a DES message. A cooperative effort on the Internet of over 14,000 computer users trying out various keys finally deciphered the message, discovering the key after running through only 18 quadrillion of the 72 quadrillion possible keys! DES originated at IBM in 1977 and was adopted by the U.S. Department of Defense. Since there is some concern that the encryption algorithm will remain relatively unbreakable, National Institute of Standards and Technology (NIST) has indicated DES will not be re-certified as a standard.

DES – See Data Encryption Standard

Digital Signature Standard – Digital Signature Standard (DSS) is the digital signature algorithm (DSA) developed by the U.S. National Security Agency (NSA) to generate a digital signature for the authentication of electronic documents. DSS was put forth by the NIST in 1994 and has become the United States government standard for authentication of electronic documents. DSS is specified in Federal Information Processing Standard (FIPS) 186.

DSS – See Digital Signature Standard

ECDSA – See Elliptic Curve Digital Signature Algorithm

Elliptic Curve Digital Signature Algorithm – The Elliptic Curve Digital Signature Algorithm (ECDSA) is used to generate a digital signature of a message digest or hash. ECDSA was approved by NIST in June 2000.

L2TP – See Layer Two Tunneling Protocol

Layer Two Tunneling Protocol – Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet Service Provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet. L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems.

Point-to-Point Tunneling Protocol – Point-to-Point Tunneling Protocol (PPTP) is a protocol (set of communication rules) that enables corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network. A company no longer needs to lease its own lines for wide-area communication but can securely use the public networks. This kind of interconnection is known as a virtual private network (VPN).

PPTP – See Point-to-Point Tunneling Protocol

RSA – RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape.

Secure Multi-Purpose Internet Mail Extensions – S/MIME (Secure Multi-Purpose Internet Mail Extensions) is a secure method of sending e-mail that uses the Rivest-Shamir-Adleman (public key) encryption system. S/MIME is included in the latest versions of the Web browsers from Microsoft and Netscape as well as most e-mail products. S/MIME is a standard to the Internet Engineering Task Force.

Secure Shell – Secure Shell (SSH), sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely connecting to a remote computer. SSH uses RSA public key cryptography for both connection and authentication.

Secure Sockets Layer – The Secure Sockets Layer (SSL) is a commonly used protocol for managing the security of a message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

S/MIME – See Secure Multi-Purpose Internet Mail Extensions

SSH – See Secure Shell

SSL – See Secure Sockets Layer

Symmetric Key Encryption – An encryption system in which the sender and receiver of a message share a single, common key used to encrypt and decrypt the message. Contrast this with public key encryption which uses two keys: a public key to encrypt messages and a private key to decrypt them. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted.

TLS – See Transport Layer Security

Transport Layer Security – Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). The TLS protocol is based on Netscape's SSL 3.0 protocol; however, TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to back down to SSL 3.0. The most recent browser versions support TLS.

Triple DES – Triple DES is a minor variation of the Data Encryption Standard (DES) developed by an IBM team around 1974 and adopted as a national standard in 1977. It is three times slower than regular DES but can be billions of times more secure if used properly. Triple DES enjoys much wider use than DES because DES is relatively easy to break with today's rapidly advancing technology.

Virtual Private Network – A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data not properly encrypted. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses.

VPN – See Virtual Private Network