ENCRYPTING MAINFRAME AND SERVER TAPES
TECHNOLOGY LETTER 12-15
Frequently Asked Questions

Technology Letter 12-15 announces a change to State Administrative Manual (SAM) Section 5345.2. By eliminating a policy exclusion in SAM Section 5345.2, state entities are now required to encrypt mainframe and server tapes or use compensating security controls. Alternatives to encryption must be approved in writing by the agency ISO, after a thorough risk analysis.

The following Frequently Asked Questions have been prepared to help state entities comply with the updates to SAM Section 5345.2.

Q1. Why is the policy exclusion to encrypting data stored on mainframe and server tapes being removed?

A1. This policy change is less about mainframe and server tapes, and more about protecting the information on all portable media, all portable storage, and all portable devices that store data which has been classified as personal, sensitive, or confidential. When data is transported outside of your secure facility, the possibility of loss is high. Should such a loss occur, and it is determined that the data meets breach notification requirements, the state's credibility suffers and costs associated with reporting are high. Financial costs can easily be in the millions of dollars and the reputation loss is incalculable.

Q2. How soon do state entities need to be compliant with this new policy?

A2. State entities must be moving toward compliance immediately. As part of this policy change, the Statewide Information Management Manual (SIMM) 70C form has been updated to provide state entities a means to certify compliance with the new policy, or, if not compliant, to submit a remediation plan.

Q3. How may a state entity determine if it needs to take action in response to this new policy?

A3. First determine if the entity uses unencrypted server or mainframe tapes which store personal, sensitive, or confidential data. If the entity does, then the entity must perform a risk analysis as outlined in SAM Section 5305.1. The risk analysis will help identify threats, assess vulnerabilities, and determine the probable consequences associated with loss or realized threat for vulnerabilities, and assist with the selection of cost-effective security measures.

Frequently Asked Questions

Q4: Is there a checklist or guidance for the security measures state entities are expected to implement?

A4: Yes. The National Institute of Standards and Technology (NIST) Special Publication 800-53, Appendix F, is a complete security control catalog that prescribes the minimum security control baseline for assets classified as requiring either a low, moderate, or high security control baseline. State entities are directed to the baseline controls for Media Protection (MP), as a starting point.

Q5: Is there an example of or guidance on acceptable compensating security controls?

A5: Yes. For example, organizations with significant staff limitations may compensate for the separation of duty security control by strengthening the audit, accountability, and personnel security controls. Note: In this example, more than one compensating control is required to provide the equivalent protection for the particular security control.

Q6: Can state entities define their own compensating controls?

A6: State entities must demonstrate every attempt was made to implement security controls from the security control catalog in National Institute of Standards and Technology (NIST) Special Publication 800-53, Appendix F.

State-entity defined compensating controls are employed only when the entity has determined, through a thorough risk analysis, that 1) the security control catalog does not contain feasible and suitable compensating controls; 2) they've documented supporting rationale for how compensating controls provide equivalent security capabilities for the information asset(s) and why the baseline security controls could not be employed; and 3) they've clearly acknowledged the risk acceptance associated with implementing the compensating control.

Q7. Our state entity has a tape library in our facility. The tapes in this library hold information classified as confidential and personal. The tape library is located in an isolated, secure room and only authorized individuals are allowed access. Does our entity need to encrypt the tapes in this library?

A7. A risk analysis will help the entity to identify threats, assess vulnerabilities, and determine the probable consequences associated with loss or realized threat for vulnerabilities, and assist with the selection of cost-effective security measures. The entity may determine through the risk analysis process that implementation of enhanced personnel and physical access controls serve as adequate compensating security controls, if the tapes never leave the isolated, secure room.

Q8. Our state entity has a tape library but we send some tapes to an offsite storage facility. This is considered best practice for disaster recovery and business continuity purposes. Do we need to encrypt the data on the tapes we send offsite?

A8. Yes. Tapes which contain information classified as personal, sensitive, or confidential and are being physically transported to and stored at an offsite storage facility must be encrypted.

Q9. What about tapes or other storage media that we need to send to a client, customer, or allied government agency? We have no dedicated courier option and the intended recipient has little to no technical expertise.

A9. It is not simply about encryption or even about technology. The goal is to protect individuals' personal and sensitive information. If it was your Social Security Number, your credit card information, or your health information, you would want the government to handle it securely. Again, it comes down to a risk analysis. We have to get our core business done, but at the same time, we must be vigilant with individuals' information. This policy update is not simply about compliance, it is about taking the risk management process, applying it to this policy, and arriving at a decision that best protects the information. It's about due diligence and due care.

ENCRYPTING MAINFRAME AND SERVER TAPES
TECHNOLOGY LETTER 12-15
Frequently Asked Questions

Q10. Why is encryption now necessary for mainframe and server tapes; didn't the exclusion for mainframe and server tapes exist because it is not feasible to encrypt them?

A10. In 2003, when the state adopted policy requiring state entities to encrypt data stored on portable media and devices, particularly laptops, it was not as feasible as it is today to encrypt mainframe and server tapes. With the rapid advances in technology, there are now many feasible alternatives to the use of tapes for data back-ups and data exchanges between business partners, such as Secure File Transfer.

In 2003, to avoid reporting costs associated with the new breach notification law, the state established a policy that required encryption of mobile devices, including laptop computers. Each year, more than 100 laptops are reported lost or stolen, many of them containing personally identifiable information. If we did not encrypt the data on the hard drives of those laptops, the state would need to send notifications practically every week.

Now, when a laptop with an encrypted hard drive is lost or stolen, we do not incur the high costs of notification or the public embarrassment. Our experience with laptop encryption has taught us that the investment up front pays off later.

Today, encryption of mainframe and server tapes, or the implementation of alternative solutions to using tapes, is both feasible and necessary to avoid costs associated with data breaches.

Encryption may not be necessary in all cases. For instance, a risk analysis may answer fundamental questions and identify the following alternatives:

- **Elimination of tapes altogether. Is that tape really needed? Check with your business partner contacts to see if they still want you to store the data on the tape.**

- **Elimination of personal, sensitive, or confidential data elements. Are the personal, sensitive, or confidential data elements still needed? If not, removal of the personal, sensitive, or confidential information may negate the need for encryption.**

- **Alternative storage methods. Can you move off tapes entirely? Other storage methods are available that use encrypted communication channels to send the data offsite for later recovery.**

- **Secure File Transfer. Can you move off tapes entirely? Automated data transfer methods are available that use encrypted communication channels to securely transfer data between business partners.**

- **Secure Facility. Are those tapes really "portable"? Tapes which never leave the confines of a secure facility, along with enhanced personnel and physical access controls, may be acceptable.**

- **Eliminate use of production data in DR exercises. Do you really need to send production data during your disaster recovery exercise? If data is anonomized, encryption is not required.**

Q11. There are many products and several encryption algorithms to choose from. Which of these are approved for use?

A11. You are correct. There are many vendor products to choose from. In some cases, you may find that you have the tape encryption capability built into a product you already own. When selecting a product or algorithm, you must be certain the product meets or exceeds the Federal Information Processing Standards 140-2.