OhioDAS Service · Support · Solutions | Office of Information Technology

IT Bulletin

Bulletin No: ITB-2008.01
Effective Date: 06/25/2008

To: Directors and Chief Information Officers of State Agencies, Boards and Commissions

From: R. Steve Edmonson, State Chief Information Officer

Cc: Sol Bermann, Chief Privacy Officer
Rex Plouck, Deputy Director

Re: Encryption and Investigatory Needs

PURPOSE

The purpose of this bulletin is to promote government accountability by providing transparency in government, preventing wrongdoing from being hidden, and deterring the abuse of encryption systems. This bulletin addresses state agency encryption practices for the security of records that are potentially subject to an investigatory effort. In the context of an investigation, state agencies would need to provide access to encrypted information to law enforcement or other investigatory agents upon a legally authorized request for a search or electronic monitoring. If a cryptographic key is unavailable to provide this access, parties legally authorized to access encrypted information may not be able to review such materials. Access should also be readily provided to those properly authorized to access encrypted content in a manner that also maintains the confidentiality of an investigation.

WHO IS COVERED

This bulletin covers state agencies, including boards and commissions, as identified in Ohio IT Policy ITP-A.1 "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services."

ACTIONS FOR STATE AGENCIES

State agencies shall establish policies and procedures to support the following actions prior to and upon presentation of a request to access encrypted information:

1. Only use encryption solutions that permit key recovery. For any solution that encrypts data for the purposes of non-disclosure, the solution must contain a key management component that allows for a highly restricted secondary means of access to encrypted information. SafeBoot encryption solutions acquired through the OIT Master License Agreement already meet this requirement.

2. Develop and document secure encryption and encryption key management practices. State agencies shall develop encryption practices consistent with state of Ohio IT policies and standards, including IT Standard ITS-SEC-01, "Data Encryption and Cryptography," and IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data." Both physical and logical controls shall be used to secure cryptographic keys. Compromise of a system storing cryptographic keys can potentially compromise all cryptographic protections used in an agency. Therefore, such systems shall be treated as higher-impact targets. Agencies shall thoroughly document their encryption practices and secure this documentation accordingly.

Office of the State CIO | 30 E. Broad Street, 39th Floor | Columbus, Ohio 43215
614.644.6446 | 614.644.9382 | State.CIO@oit.ohio.gov

Robert Blair, Director
Stuart R. Davis, Assistant Director/
State Chief Information Officer

3. Designate encryption points-of-contact. The agency chief information officer or lead IT administrator shall have access to cryptographic keys and shall serve as an encryption point-of-contact. In addition, the agency shall appoint one or more encryption points-of-contact who shall have access to cryptographic keys. Ohio IT Policy ITP-B.1, "Information Security Framework," requires agencies to subject all personnel with access to system assets to a vetting process commensurate with the system assets' risk assessment. Personnel with access to cryptographic keys or sensitive information require thorough vetting.

4. Identify and authenticate the investigator and the request. State agencies shall maintain cryptographic keys in such a manner that the investigatory agency may confidentially access any encrypted data. The investigatory agency must formally notify the state agency of the investigation: the Office of the Inspector General must present a formal notice of investigation; the Ohio State Highway Patrol, the Bureau of Worker's Compensation, or the Bureau of Criminal Identification must present a search warrant. Requests and warrants for access to encrypted information, including those requests made by outside law enforcement agencies, shall be routed through the Ohio State Highway Patrol or the Office of the Inspector General. Once the request or warrant has been validated by the State Highway Patrol or the Office of the Inspector General, the investigatory agency shall forward the request to an encryption point-of-contact within the agency describing why access to the encrypted information is necessary and specifying what use will be made of the information. A request or warrant to access a computer, removable media or other IT asset includes by definition the means to access all information on the IT asset including encrypted information. If the agency chief information officer is the subject of the investigation, the investigatory agency shall forward the request to another agency encryption point-of-contact. The individual or entity requesting access to encrypted information must be legally authorized to access encrypted information. Apart from the state agency that owns the data, only the following agencies have the investigatory powers to access encrypted information:

- Ohio State Highway Patrol;
- the Attorney General's Bureau of Criminal Identification and Investigation;
- the Bureau of Workers' Compensation; or
- the Office of the Inspector General.

Unless otherwise provided by law, information identified under a subpoena issued by a civil court, tribunal, officer or other authority with jurisdiction over a civil proceeding may be released by state agencies upon sufficient service of the subpoena. The cryptographic key shall not be released unless such action is specifically ordered in the subpoena. If a subpoena pertains to information that is required to be confidential by law, state agencies shall take all reasonable steps to secure a protective order from a court of law to provide the maximum protection possible for the confidential information.

5. Identify the target data. The investigatory agency and the state agency that received the request shall identify the information necessary to fulfill the request, such as whether the request applies to data associated with a particular user, device, or a defined time period. Agencies shall limit access to only those records specified in the request.

6. Provide access to decrypted information. The chief information officer or other designated encryption point-of-contact shall securely provide the investigatory agency access to the decrypted information. Access to decrypted information shall be provided to the investigator for a period of time necessary to copy the information to another device or media. To ensure access to encrypted records is possible, state agencies shall maintain cryptographic keys for records in accordance with the relevant retention schedule of the record being encrypted. State agencies shall also ensure that backup and recovery of cryptographic keys are a part of the agency's business continuity plan.

7. Report illegal activity and wrong-doing. If an encryption point-of-contact identifies evidence of illegal activity or serious wrong-doing related to an investigation involving the use of cryptographic keys or decrypted information, the encryption point-of-contact shall refer to the Governor's memo on "Procedures for Notification of Employee Wrongdoing and/or Suspected Illegal Activity" for further action and shall alert

the appropriate investigatory body. State agencies shall develop and maintain a statement of responsibility indicating that the party that obtains lawful access to cryptographic keys or decrypted information per an investigatory request shall be liable for the misuse of such materials. State agencies shall adopt a procedure requiring an investigatory agent to sign the statement of responsibility per a request.

ACTIONS FOR INVESTIGATORY AGENCIES

In addition to following the process outlined in "Actions for State Agencies," investigatory agencies will collect and secure sensitive information to be used in an investigation. Such agencies shall ensure that the investigation disrupts neither the data's integrity or confidentiality, nor breaches the confidentiality of the investigation to outside parties. State agencies shall monitor the use of the cryptographic materials and revoke access once it is no longer necessary, as determined by the investigating authority.

ACTIONS FOR THE CHIEF PRIVACY OFFICER

The Chief Privacy Officer shall develop procedures for the secure submission of agency encryption points-of-contact to the Chief Privacy Officer. The Chief Privacy Officer shall also maintain the encryption points-of-contact list and provide such information to investigatory agencies upon request.

AUTHORITY AND REFERENCE

ORC 125.18; ORC 149.011; Executive Order 2007-013S; Ohio IT Policy ITP-B.1, "Information Security Framework"; Ohio IT Standard ITS-SEC-01, "Data Encryption"; Ohio IT Bulletin ITB-2007.02, "Data Encryption and Securing Sensitive Data"; Governor's memo on "Procedures for Notification of Employee Wrongdoing and/or Suspected Illegal Activity"

INQUIRIES

Direct inquiries about this bulletin to:

Chief Privacy Officer
Ohio Office of Information Technology
30 East Broad Street, 39th Floor
Columbus, Ohio 43215
Telephone: 614-644-9391
E-mail: Chief.Privacy.Officer@oit.ohio.gov