Description of document: President's Council on Integrity and Efficiency Information (PCIE) Information Technology Investigations Sub-Committee Report: Key Escrow Management and File Encryption Challenges for the Federal Inspector General Community, June 2008

Requested date: 24-November-2013

Released date: 09-December-2013

Posted date: 27-January-2014

Source of document: Council of the Inspectors General on Integrity and Efficiency
1717 H Street, NW, Suite 825
Washington, DC 20006
Fax: (202) 254-0162
Email: FOIASTAFF@cigie.gov

Council of the
INSPECTORS GENERAL
on INTEGRITY and EFFICIENCY

December 9, 2013

Subject: Log No. 6330-2014-8

This letter responds to your Freedom of Information Act (FOIA) request, dated November 24, 2013, to the Council of the Inspectors General on Integrity and Efficiency (CIGIE). Your request was received on December 2, 2013. You requested a copy of the PCIE Information Technology Investigations Sub-Committee Report, Key Escrow Management and File Encryption Challenges for the Federal Inspector General Community, June 2008.

We are releasing 7 pages of responsive documents. Pursuant to FOIA, certain information has been redacted as it is exempt from release.

You have the right to appeal CIGIE's response by writing to the Council of the Inspectors General on Integrity and Efficiency, 1717 H Street NW., Suite 825, Washington, D.C. 20006-3900. Your appeal must be received within 45 days of the date of this letter. The outside of the envelope should be clearly marked "FOIA APPEAL."

Sincerely,

Mark D. Jones
Executive Director

Enclosure: Documents

Key Escrow Management and File Encryption Challenges for the Federal Inspector General Community

June 2008

Prepared and Presented by President's Council on Integrity and Efficiency Information Technology Investigations Sub-Committee

Background

In recent years, the federal government has taken its share of criticism on the safeguarding of sensitive data. Events which have inspired the focus of public attention included the theft of a laptop containing millions of names and personnel data from a Veteran's Administration (VA) employee in May 2006. At the time, reports detailed that the thief had the names and Social Security numbers of every veteran discharged after 1975. It was the largest Social Security numbers breach ever -- the VA disclosed that approximately 26.5 million veterans were at risk of identity theft.

Additionally, other agencies charged with collecting personal information had security problems. In response to public inquiry, the Commerce Department determined that 1,137 laptops distributed within its 15 operating units were either lost, stolen, or missing from 2001 to 2006. Of these 1,137 laptops, 249 contained personally identifiable information (PII).

Between 2003 and 2006, nearly 63,000 cyber incidents were reported to the Homeland Security Department's U.S. Computer Emergency Readiness Team. In 2007, these cyber incidents exploded. The federal government is placing an increased effort in minimizing and preventing future attacks. The Wall Street Journal recently reported President Bush proposed a $6 billion budget to build a system to protect U.S. communication networks from attacks. This is in response to some recent information security news:

The Department of Homeland Security counted 37,258 attacks on government and private networks last year, compared with 4,095 in 2005 (Source: Wall Street Journal).

Auditors of the Department of Energy's interconnected networks called 132 security breaches serious enough to report to law enforcement in FY06 – 22% more than in the prior year (Source: Federal Computer Week).

Foreign hackers are increasingly seeking to steal Americans' health care records, according to a Department of Homeland Security analyst. (Source: Federal Computer Week).

Furthermore, new ways to manage the IT infrastructure within federal agencies have made access to government data even more challenging. For example, in one instance cited by the PCIE IT Subcommittee, the Department of Education (ED) contracted its IT functions and data storage to a private contractor. When Inspector General (IG) personnel requested access to computer information, the contractor did not permit access until after the IG obtained a subpoena. By not allowing IG employees access to Department of ED data, this was in direct violation of the IG Act[1]. Even more complex cases have arisen when companies performing data storage commingled government customer data with other customers. In those cases, there is no clear legal precedence as to whether or not a subpoena is required.

OMB Memorandum M-06-16, June 23, 2006, recommended all departments and agencies:

> 1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
>
> 2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
>
> 3. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
>
> 4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

OMB Memorandum M-06-16 also stated:

> Most departments and agencies have these measures already in place. We intend to work with the Inspectors General community to review these items as well as the checklist to ensure we are properly safeguarding the information the American taxpayer has entrusted to us. Please ensure these safeguards have been reviewed and are in place within the next 45 days.

OMB Memorandum M-07-16, May 22, 2007, re-iterated the requirements for safeguarding against and responding to the breach of personally identifiable information (PII). Despite the National Institute of Standards and Technology

[1] Section 6, authority of Inspector General; information and assistance from Federal agencies; unreasonable refusal; office space and equipment (a) In addition to the authority otherwise provided by this Act, each Inspector General, in carrying out the provisions of this Act, is authorized (1) to have access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to the applicable establishment which relates to programs and operations with respect to which that Inspector General has responsibilities under this Act.

(NIST) checklists and the recommendations from OMB for departments and agencies to take actions regarding encryption and other security safeguards, there is no easy way to identify and prevent all system vulnerabilities. According to testimony presented at the Senate Homeland Security and Governmental Affairs Committee on information security on March 12, 2008, only 4 of 24 federal agencies have implemented acceptable Federal Information Security Management Act of 2002 (FISMA) compliance system security safeguards. The best strategy to mitigate risk is to use common sense and a combination of several methods, known as a layered defense. Common methods to prevent threats are monitoring what programs are running, installing anti-spyware, firewalls, network monitors, intrusion detection, two-factor authentication, and biometric identification. With the escalating security threats, departments and agencies, with the assistance of their IGs, must consider moving forward quickly.

Each government organization has the need to protect sensitive personally identifiable information, and should base the management of those systems in an organizational policy statement. Strong encryption using cryptographic systems can be used, but can also be compromised by lax and inappropriate human actions. Highly unusual events should be noted and reviewed as possible indicators of attempted attacks on the system.

Cryptographic mechanisms are one of the strongest ways to provide security services for electronic applications and protocols and for data storage. Federal Information Processing Standards (FIPS) and NIST Special Publications specify cryptographic techniques for protecting sensitive unclassified information. Key management provides the foundation for the secure generation, storage, distribution, and destruction of keys. NIST Special Publication 800-57, Recommendation for Key Management, Part 2: Best Practices for Key Management Organization, advises developers and system administrators to use industry best practices associated with key management. OMB guidance to federal agencies on Data Availability and Encryption, November 26, 2001, stated that agencies must address information availability and assurance requirements through appropriate data recovery mechanisms such as cryptographic key recovery. The key management policy should prescribe, for each element, any roles, responsibilities, facilities, and procedures necessary for all organizational elements to backup and recover critical data, with necessary integrity mechanisms intact, in the event of the loss of the operational copy of cryptographic keys under which the data is protected. Key backup and recovery is normally the responsibility of the central oversight authority, or its organizational equivalent, although mechanisms to support recovery are likely to be included in client node, service agent, and especially key processing facilities, or their organizational equivalents.

Challenge

Agencies are required to proactively implement appropriate information security controls to support the mission in a cost-effective manner, while managing evolving information security risks. The FISMA requires agencies to integrate information security into their capital planning and enterprise architecture processes. OMB Circular A-130, Management of Federal Information Resources, November 2000, places the burden on federal managers to ensure that management, operational, and technical safeguards or countermeasures are prescribed to protect the confidentiality, integrity, and availability of the system and its information. The Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 2004, increased identification security and interoperability, requiring increased authentication for federal employees and contractors for access to federal facilities and information systems.

As with any policy decision, there are often times unintended consequences of otherwise well-intentioned actions. For example, the 45-day implementation requirement imposed by OMB in 2006 left little time for careful consideration of the impact of encrypting government data. In the case of the IG, the encryption and security demands did not include anything regarding the importance of developing key management policy availability before deploying encryption access to all data as required by the IG Act of 1978 as amended. OMB Memorandum M-06-16 refers to the IG as being an enforcement arm to ensure compliance. However, the guidance did not address the overall impact that data encryption will have on IG offices, nor did it stress the importance of developing and implementing proper enterprise-wide key escrow policy and practices. A recent data call to the IG community and federal Chief Information Officers (CIO) Council for existing key escrow policy produced only a few responses. IG community responses varied from extremely detailed and robust key escrow policies to a one page high-level document.

Department of Defense chose to implement a key escrow system for business, law enforcement, and counterintelligence requirements. The key stored in this key escrow system, any part of the key, or information necessary to access the extracted key are referred to as the "escrowed key". Their policy delineates how the escrowed key is stored, how authorized personnel can submit requests for copies of the escrowed key, how it is retrieved, and how it is delivered to an authorized requestor. It also specifies how the escrowed key is protected during each of these activities.

Public key cryptographic mechanisms support secure communications by providing security services such as integrity, authentication, and confidentiality. Encryption of agency data presents risks to the availability of information needed by the agency to reliably meet its mission. Specifically, without access to cryptographic key(s) needed to decrypt information, the agency risks losing access to its valuable information. Additionally, confidentiality policy within any key management is of concern for all IGs with regard to ensuring operational security during ongoing investigations. Access to encrypted data must be available to investigators without the individual under investigation being alerted. The encryption methods must provide a data recovery service and support data recovery for business and law enforcement requirements.

By placing more weight on the secure storage of sensitive data, policy makers have inadvertently hampered the efforts of IG officials in conducting their mission. The major weakness in this area is that IT policy for key management does not describe the goals, responsibilities, and overall requirements for the management of cryptographic keying material used to protect private or critical facilities, processes, or information.

Recommendations

The IGs need to conduct meetings with agency officials to ensure that agencies are diligently protecting sensitive personally identifiable information, and basing the management of those systems in an organizational policy statement. Specifically, this subcommittee recommends immediate action by the IGs to address system security and privacy concerns as follows:

1. Recommend to CIOs that they to diligently protect sensitive personally identifiable information, and base the management of those systems in an organizational policy statement.

2. Recommend to CIOs that they work in conjunction with the IG to implement appropriate information security controls to support the mission in a cost-effective manner, while managing evolving information security risks.

3. Conduct meetings with CIOs to structure IT policy that incorporates compliance with the IG Act, so that the IG has access to all records, reports, audits, reviews, documents, papers, recommendations, or other material available to accomplish its programs and operations. This access needs to be codified in departmental or agency policy action.

4. Recommend to CIOs that they include language in all contracts and purchasing documents for IG personnel access to records and system data for all contractor-owned systems that contain federal data. IG personnel should not have to obtain a subpoena to gain access to computers with federal data.

5. Recommend to Contracting Officers that they require all contractors performing data storage to agree that government customer data will not be commingled with other customer data.

6. The IGs need to ensure management establishes a key management policy that describes the goals, responsibilities, and overall requirements for the management of cryptographic keying material used to protect private or critical facilities, processes, or information. Key management policy should:

a. State the security objectives that are applicable to and expected to be supported by the Key Management Infrastructure (KMI). The security objectives should include the identification of:

    i. The nature of the information to be protected (e.g., financial transactions, confidential information, critical process data);
    ii. The classes of threats against which protection is required (e.g., the unauthorized modification of data, replay of communications, fraudulent repudiation of transactions, disclosure of information to unauthorized parties);
    iii. The Federal Information Processing Standard 199 (FIPS 199) impact level which is determined by the consequences of a compromise of the protected information and/or processes (including sensitivity and perishability of the information);
    iv. The cryptographic protection mechanisms to be employed (e.g., message authentication, digital signature, encryption);
    v. Protection requirements for cryptographic processes and keying material (e.g., tamper-resistant processes, confidentiality of keying material); and
    vi. Applicable statutes, and executive directives and guidance to which the key management infrastructure and its supporting documental shall conform.