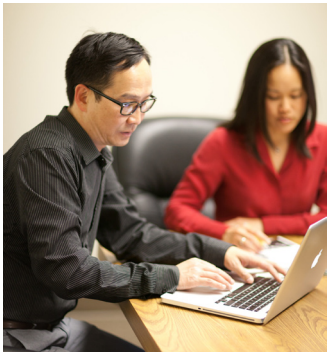
Adobe solutions for protecting personally identifiable information

Government agencies can raise security for sensitive data using Adobe® LiveCycle® Rights Management ES



The U.S. government has experienced a number of high-profile data security breaches involving the loss of personally identifiable information (PII) in the past few years. PII is any piece of information that can potentially be used to identify, contact, or locate a specific person, such as a driver's license number, email address, telephone, or Social Security number.

As risks have escalated, they have shifted from mostly external threats to more internal threats. To help address this issue, the president signed an executive order in May 2006 creating the Federal Identity Theft Task Force. Several of the task force's interim recommendations focus on the need to increase data security, improve government agencies' ability to respond to data breaches, and reduce the risk of threat to PII. This guide explains how the Adobe LiveCycle Rights Management ES module can help agencies proactively act on these recommendations.

Guidance from the Office of Management and Budget

In June 2006, the Office of Management and Budget (OMB) issued guidance to federal agencies to eliminate weaknesses in security control mechanisms and improve privacy protection in all federal departments and agencies. The OMB recommends that all departments and agencies take the following actions:

1. Encrypt all data on mobile computers and devices that carry agency data, unless the data is determined to be nonsensitive.
2. Allow remote access only with two-factor authentication, where one factor 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 reauthentication after 30 minutes of inactivity.
4. Log all computer-readable data extracts from databases holding sensitive information and verify that each extract that includes sensitive data is erased within 90 days or that its use is still required.

LiveCycle Rights Management ES provides a comprehensive solution for agencies looking to reduce their information risk from PII leakage, loss, or breach. To address recommendation 1, LiveCycle Rights Management applies persistent protection for documents and all document versions, ensuring that mobile computers containing sensitive agency PII are always protected. For recommendation 4, agencies can use LiveCycle Rights Management to apply a policy to PII data when it is extracted from databases. Access rights can be revoked after a defined time period, whether it is a set time of 90 days or until access is no longer required. For recommendations 2 and 3, Adobe partners who specialize in identity management and virtual private network (VPN) technologies can help provide a comprehensive solution.

In addition to its high-level recommendations, the OMB also recommends following the National Institute of Standards and Technology (NIST) checklist outlining how agencies can better protect the access and storage of remote information:

- Identify and confirm PII protection needs.
- Verify adequacy of organizational policy.
- Implement protections for PII being transported and/or stored off-site.
- Implement protections for remote access to PII.

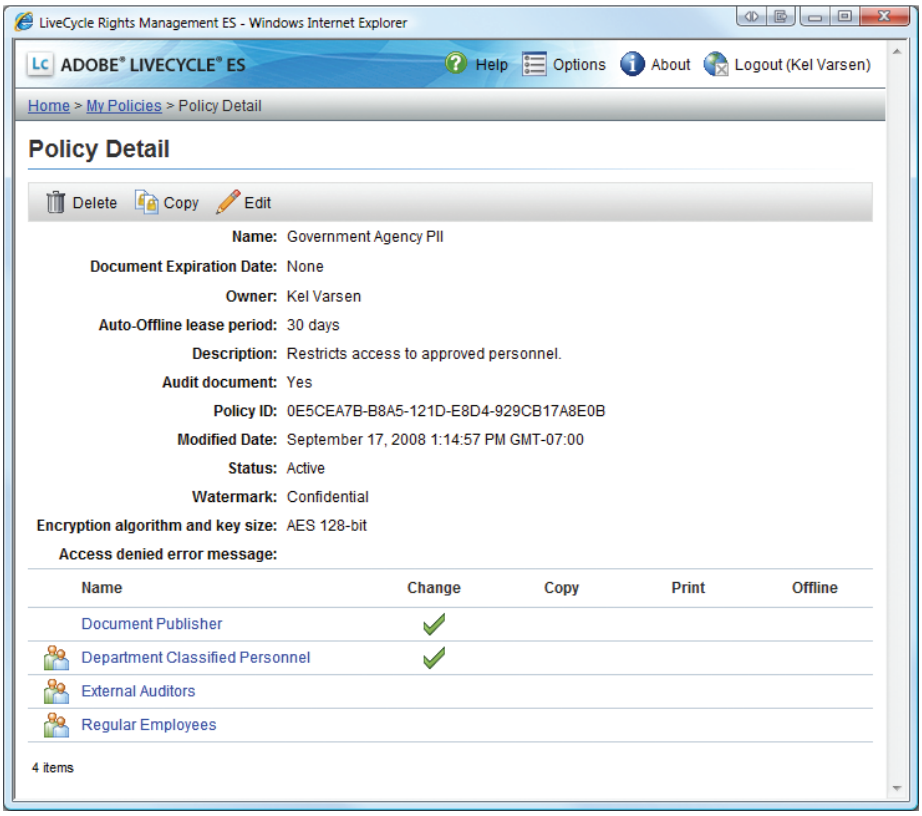
The need to address this issue has become more acute as employees increasingly access information remotely, at home or on the road, and typically outside the agency firewall. Information is becoming more and more dynamic. It's constantly moving throughout the organization from databases, to applications, to content management systems and storage, and ultimately out to endpoints and mobile devices.

The OMB memorandum indicates that information must be protected in all states: in storage, at rest, in motion, and during use. It is imperative that federal, state, and local government agencies address the accessibility of information with solutions that provide protection that is integrated with the information itself. LiveCycle Rights Management ES provides the information-centric security needed to protect data, regardless of where it resides, where it moves, or how it is stored.

Discover and identify high-impact PII data

The first NIST checklist item directs agencies to discover where sensitive PII information resides and to identify high-impact data. High-impact data represents the hot spots where agencies must focus their time and resources first to reduce the risk of PII data loss. After the discovery phase is complete, the agency should confirm or modify its risk assessment, as required. A government organization can identify areas where high-impact PII information resides in a number of ways. For instance, sensitive data typically resides at rest in enterprise content management (ECM) systems, databases, and centralized repositories such as file systems. However, hot spots can also be found in motion, in emails or email attachments, instant messages, and mobile devices. These are areas that are often not protected, leaving agencies vulnerable to attack as data is in motion or transit.

Technologies that help classify data can be used in conjunction with LiveCycle Rights Management ES to provide a complete information policy management framework. Using this approach, you can automate protection schemes based on the sensitivity level of the documents. As you define high-impact PII, you establish a starting point for deploying rights management based on enforcement policies.



Access privileges are based on the individual's role or rank within the agency.

Author and implement PII policies

When the discovery phase is completed and you have a blueprint of your PII hot spots across the organization, the next step is to create and tune PII-specific policies to help control the flow of information. You can enforce persistent protection by linking the classification of the data specific rights management policies.

LiveCycle Rights Management ES offers departments and agencies flexibility in the way policies for PII protection are created, managed, and modified so that each group can develop policies best suited for its particular situation. A government employee can create policies, or a central authority can deploy policies to a group of users. Policies can also be automatically applied to documents in a workflow using watched folders. Based on the sensitivity level of the information, policies dictate the rights users or groups have to view, print, or edit a particular document. If information in the intelligence community is considered classified, rights can be assigned according to the potential viewer's role within the agency.

Using Adobe policy sets, administrators can delegate who can create and manage shared policies. This feature also enables agencies to control which policies each individual or workgroup can use. These policies can also be changed, revoked, or modified on the fly, allowing turnover among contractors and other temporary employees or a quick response to dynamically changing information.

Protect and control PII using encryption

Encryption controls can protect content as it is accessed remotely or transported. LiveCycle Rights Management ES uses Federal Information Processing Standard (FIPS)-compliant encryption controls to protect data, whether it is at rest, at a remote site, or in motion. Technologies that focus on access control alone cannot provide protection that remains with the information wherever it goes. LiveCycle Rights Management applies encryption at the source: to the information itself. It also works with access controls in ECM systems to extend in-depth defense. In addition, LiveCycle Rights Management has the capability to alter, revoke, or change controls at any time—online or offline.

Additional protections for remote access of PII

It is also vital to have procedures for accessing PII from remote locations via a VPN. In cases where it is appropriate to download PII to a remote location, the information must be encrypted at the remote location.

Protect PII with LiveCycle Rights Management

Overall, agencies that are striving to adhere to the OMB recommendations must be proactive about securing the most sensitive and risky PII that resides throughout the agency IT infrastructure. LiveCycle Rights Management protects information persistently, regardless of its location, based on policies that reflect the inherent sensitivity of the data and that identity those trying to access it. Other technologies, including perimeter-focused tools, aim to ensure that hackers cannot gain access to the information. However, those technologies do little to stop someone who already has access to the data from releasing it, maliciously or unintentionally.

LiveCycle Rights Management is part of a comprehensive information risk management strategy that agencies can implement using people, process, and technology to ensure effective internal adoption and protection of PII assets.

For more information

For more details about Adobe solutions for protecting personally identifiable information, visit *adobe.com/products/livecycle/rightsmanagement/* and *adobe.com/government/solutions/secure_info_sharing/*.

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

Adobe, the Adobe logo, and LiveCycle are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other trademarks are the property of their respective owners.

© 2013 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

95011598 1/13