

Feds Seek Enterprise-wide Content Management

Federal agencies are struggling to increase information security, comply with regulatory mandates, transition retiring workers and cut IT costs – while simultaneously increasing operational efficiency.

Mandates such as Circular A-123 from the Office of Management and Budget and the Federal Information Security Management Act (FISMA) are straining their technical and human resources. As a result, many federal agencies are looking for enterprise content management solutions that can help them cost-effectively manage and automate traditionally paper-based processes and increase the security of their electronic documents. Award-winning enterprise content management solutions from Oracle offer federal agencies the most usable, manageable and hot-pluggable platform for simultaneously improving information accessibility and security.

By allowing customers to create and manage agency-wide standardized information management processes, Oracle Content Management enables federal agencies and departments to better comply with regulations, protect sensitive information, increase operating efficiency, reduce data processing costs and improve the quality of information available to government employees, vendors and citizens. Oracle content management solutions can also greatly improve inter- and intra-agency information sharing. Oracle Content Management is part of Oracle Fusion Middleware, the industry's most comprehensive and integrated middleware for delivering a clear path to service-oriented architecture (SOA). Its open architecture can be easily integrated with legacy applications and data sources, and can be used to automate and streamline cumbersome manual processes.

Setting Oracle Apart

Universal Content Management (UCM), Oracle's

Oracle Content Management Benefits

By leveraging Oracle content management solutions, federal agencies can:

- Streamline agency compliance processes by distributing the process documentation, control, review and testing tasks to process owners;
- Smooth the auditing process by providing full audit trails of documentation changes as well as test and remediation results;
- Optimize controls by centrally creating test plans for control sets that apply to multiple agency work groups;
- Extend support for other compliance initiatives;
- Provide easy access to documentation for internal and external auditors;
- Satisfy security and retention management requirements;
- Improve communication by using batch-driven workflows and automatic e-mail notifications of tasks and tests to be performed.

flagship content management product, can be used to optimize documentation-intensive compliance activities, support eGov initiatives, enhance information-sharing and accelerate content-related work processes. UCM unifies the management of Web content, documents, and digital assets and enables government organizations to reduce both integration and operational costs. Its easy-to-learn user interface minimizes training costs and speeds broad end-user adoption.

Oracle Universal Records Management (URM) was the first solution to receive agency-wide DoD 5015.2 Chapter 2 and Chapter 4 certification for electronic and physical records management. URM allows for the automation of records management policies such as retention periods, dispositions and audit holds, at any location and within any repository. URM's integration with UCM and popular third-party repositories, security and enterprise applications makes widespread deployment of standardized records management

Content management is increasingly being used to help manage the lifecycle of unstructured content such as images, documents, reports and web sites, while maintaining the integrity of that content and controlling access to authorized personnel, whether they are located within or outside the organization.

policies quick and easy. In addition to supporting the Intelligence Community Metadata Standard for Publications (IC MSP), Oracle content management solutions provide a platform for rapidly deploying applications that meet security guidelines, including those outlined in the Director of Central Intelligence Directive (DCID) 6/3 manual, which imposes strict controls for the protection of IT systems containing intelligence data. Oracle content management products can also fulfill Protection Level 3, Community of

Interest 4(PL3 COI4) security requirements, which restrict data access to authorized users, and leverages next-generation security tools for data protection.

Oracle Information Right's Management (IRM) advances information security through technology that can secure and track sensitive digital information even when it moves beyond organizational boundaries. Unlike conventional information management products that can only manage documents while they remain stored in centralized repositories, Oracle IRM uses encryption and rights management to protect information that has been copied or sent beyond the repository. IRM can manage every copy of an organization's most sensitive information, regardless of where it's stored and used – including on desktop computers, laptops, wireless mobile devices and removable media. IRM can also enable organizations to reduce the danger of data theft, retiree's retention of sensitive data and inadvertent misdirection of sensitive emails. Its effective user rights model secures and locks sensitive information and can be configured to verify that stakeholders are always viewing the latest versions of time-sensitive documents.

For more information, please visit

www.oracle.com/goto/contentmanagement

or call 1.800.633.0584.