opentext™

Information Governance and Security Solutions

The interdependent mission objectives of US Department of Defense and Intelligence Community (DoD/IC) Agencies are supported by a highly complex mix of operational processes and information systems that must interoperate effectively to meet combined and disparate requirements. With the rapid evolution of technology and exponential growth of data being created, effectively managing processes and supporting information in an open yet secure manner is a critical challenge.

opentext™

Table of Contents

Introduction 3

Insider Investigation Scenario 4

Investigation Support Solution Highlights. 5

Enterprise Interoperability and Security Context 6

Profiling of information 7

Metadata Driven Access Schemas 8

Leveraging Analytics within Information Governance and Security Operations 9

Process Governance and EIM 10

Summary of Information Governance and Security Solution Benefits 12

Introduction

Typically, when we think of security, we think mostly of external or internal threats, which require an explicit or inadvertent action to compromise the integrity of an organization's information. In the context of information governance and security, we need to flip this perspective and consider the information itself to be the object which may catalyze a security event. Likewise, information serves as a catalyst for action across the DoD/IC operational scope, from budget management to supply chain, cybersecurity to mission execution. Based on these perspectives, the OpenText solution approach begins with information itself, then supporting infrastructure, then usage within operational context and the individuals that leverage information to fulfill mission objectives.

The focus of this briefing is the combination of complementary governance and security management capabilities which form an 'information and consumer aware' solution set. The capability set includes: Process Governance, information profiling, automated content classification, records management, along with flexible yet highly secure information access controls. In support of the overall solution set are sophisticated information profiling and access monitoring capabilities, which can be employed to track what information is being utilized, along with detection of insider and other cybersecurity threats. With profiling in place, far more information can be securely shared within and across agencies, as well coalition partners, increasing operational effectiveness. The capability set can be employed as a stand-alone solution and/or embedded within any front end application in use by a particular Agency.

In order to meet the complex and dynamic access requirements in support of DoD/IC 'information consumers' we describe below three types of access schemas: Role, Activity and Subject Matter based. Role based access hinges on 'who you are' in an organization, a fairly simple hierarchical model. Whereas 'activity based access' is related to 'what you do' (mission, program or investigation assignments, etc.), so this is a time sensitive, more complex model. Lastly, 'subject matter' based access hinges on an individual user's area of expertise, with education and training considered, thus providing a multi-faceted information focused approach.

Whether via interoperability with agency front end applications and/or automated profiling, the operational context of information is always maintained. With operational context linkage, information is available at the appropriate process point, within the application in use. This eliminates time consuming navigation through a myriad of source applications to get data needed to complete a process.

To better describe the solution set in action, we'll focus on a scenario that involves the investigation of an 'insider' that has ex-filtrated Unclassified Technical Information (UTI), which if compiled could reveal information considered classified. Investigators, attorneys and other participants have access to information based on their organization, job roles, activities performed in support of the investigation, and their areas of expertise. Security clearance levels of participants are always utilized when determining access to investigation related information.

FIGURE 1

Complex roles and information access needed to conduct an investigation.

- The **Investigator** has full access and control of all case related information (evidence) including Classified/Secret materials, throughout the specifici process steps of the investigation.
- The **Investigations Lead** has narrowed accessto case related information, i.e. will not include privacy information. The Lead will have access to Classified/Secret materials, he/she will approve finalized Case Files and disposition.
- The **Case Attorney** will have access to case related information during case finalization and disposition steps. Metadata/search access will not include privacy information. Private and Classified/Secret information will be redacted in Document Views.
- The **Supervising Attorney** will have limited access to case related information during case finalization and disruption steps. The Supervising Attorney access will not include privacy or Classified/Secret information, he/she will also approve final Case File and dispostion.

Insider Investigation Scenario

Fred Showthem is an engineer with a DoD contractor that supports remotely piloted aerial vehicle operations, aka drones. He has expressed to co-workers that he's been very disturbed by the alleged use of armed drones to strike at Americans involved in Jihadi terrorist activities overseas. It is alleged that his concerns motivated him to ex-filtrate unclassified technical information related to the Global Hawk program, including a wide array of capabilities documentation, video surveillance files and sensor data from operational missions. It is alleged that he then provided this information to a US adversary with the intent to compromise the effectiveness of drone missions.

Evidence gathered to date:

- Mr. Showthem downloaded a wide variety of drone related documentation and mission data.
- As evidenced by systems logs, he performed downloads from a number of systems including: SAP®, Oracle® EBS, Microsoft® SharePoint®, Network File Shares and other content repositories.
- Mr. Showthem then used his company's email system to attach downloaded files, which he then forwarded to his personal email account.
- As evidenced by open and all-source intelligence, some of the information downloaded by Mr. Showthem appeared on websites and on US adversary systems.
- During an initial interview, Mr. Showthem maintains that he simply was forwarding information needed to work from remote offices. He indicated that detection of information he downloaded on external systems was purely coincidence.
- Until the investigation concludes, Mr. Showthem's system access has been removed and he has been placed on administrative leave.

Investigators must determine whether or not the evidence indicates that charges should be brought, and whether a compilation of the information released could be used to create classified information. Whether or not intended, the latter would result in a more severe charge under applicable law.

Investigation Support Solution Highlights

Metadata Driven Information Governance and Security: Metadata drives the management of complex access and controls needed for investigation processes. Metadata is employed in the gathering, correlation and securing of relevant evidence in support of the investigation. Metadata is essential in establishing 'chain of custody' of evidence gathered, which will be required should charges be brought against Mr. Showthem. Electronic evidence includes: emails, documents and other content ex-filtrated, system logs, surveillance and witness interview videos. Physical evidence tracking can also be managed within the solution, including related metadata.

Tagging of Information Objects: Metadata tagging of each information object (content files) related to the investigation is key to the management of those objects as evidence. Whether within existing systems or created as part of the case processes, metadata along with supporting audit logs will need to be provided should charges be brought. Tagging is a prerequisite to records (evidence) and information lifecycle management, along with general compliance requirements.

Metadata Driven Access Controls: Complex controls are applied across the participant's scope of information access needed to complete investigation assignments. Access limits can be set from viewing of metadata/search fields to documents types and security classifications, to specific content within a document. The ability to add document versions, view a document before it is completed by an investigation participant, etc. can also be limited for specific participants.

Leveraging Analytics for Information Governance and Security Optimization: For the investigation, analytics will assist in the gathering of evidence by helping to spot relationships between information and alleged exfiltration exposure. Visualizations and reports can also be used in the presentation of evidence should a trial be required.

Process Governance and EIM: For the investigation, process is critical to consistency and compliance for the information (evidence) captured. As 'activity based access' will be assigned as part of investigation launch, Process Governance can be employed across required systems to ensure proper access is implemented. At various points of the investigation, access for specific participant types can be limited or removed automatically, based on 'process state.' At investigation close, all activity based access will be automatically removed.

CONTENT SUITE

- Content Metadata drive design
- Sophisticated Content Creation, Collaboration, Approval, Search, Discovery and Hold capabilities
- Interoperate/embed into any application or portal
- DoD5015.02 RM certified for SAP, Oracle EBS and SharePoint content management

ANALYTICS SUITE

- Enterprise Data Model driven design
- Rich set of data Visualization and Analysis tools
- User adjustable views
- Content-centric analytics capabilities
- Embed into OpenText EIM Suites or any application

PROCESS SUITE

- Process Model driven design, BPMN 2.0 compliant
- Comprehensive process management and measures ensure continuous operational improvement
- Operation areas can adjust processes when needed
- Broad range of pre-built integrations

EXPERIENCE SUITE

- User Persona driven design
- Dynamic aplication access
- Users can tune app behaviors to device or other preferences
- Connect to any app or portal

FIGURE 2

Connecting Operations Processes and Information.

OpenText Enterprise Information Management (EIM) Services

Enterprise Interoperability and Security Context

OpenText solutions are driven by underlying metadata, which enables 'information aware' governance, process integration and security. Based on geo-political and organizational events, real-time adjustment of metadata profiling and controls help keep pace with ever changing mission needs while maintaining the operational context of information.

OpenText Enterprise Content Management (ECM) solution components are DoD 5015.02 certified, following prescribed metadata models specified in the certification requirements. This includes the Security Clearance metadata schema and controls required to meet the specifications of that certification.

For maximum flexibility, OpenText ECM solutions include COTS integration with source systems, such as Oracle EBS, SAP, email and SharePoint, along with open integration to other applications via REST APIs and/or WEB Services. This integration enables:

- Changes in application-specific information and user access profiles are automatically shared across EIM connected solutions without manual access profile updates within specific systems
- Consumers can create and access information in operational context within a front end application security framework, rather than spend time getting multiple system security authorizations
- Metadata driven, multi-layer security that helps prevent unauthorized access to information
- Proactively monitoring anomalous information use (excessive printing, downloads, etc.) for authorized access

Whether information is related to an investigation, maintenance and repair operations or recruitment onboarding processes, content (both structured and unstructured) fuels the daily operational activities that support mission objectives. Embedding EIM within key systems makes content accessible in operational context across processes, applications, and people. In turn, support of role, activity and subject matter based access security described below can be efficiently maintained.

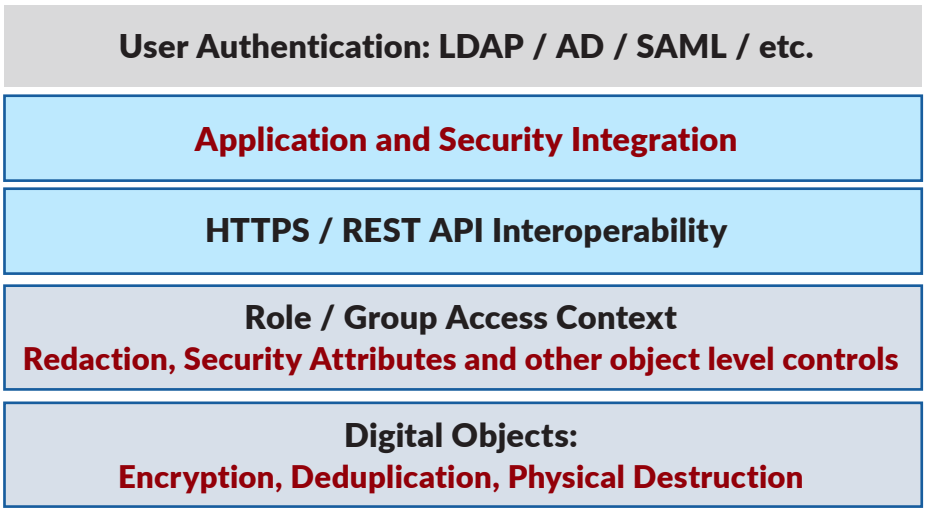


FIGURE 3

Metadata driven interoperability and security is key to managing complex access requirements for investigation participants. Metadata is employed in the gathering, correlation and securing of relevant evidence in support of the investigation, then providing proof 'chain of custody' of evidence gathered.

Profiling of information

A critical success factor for EIM solution deployment is the ability to locate information quickly and easily, with the assurance that the information is relevant, complete and accurate. In essence, EIM solutions enable a virtual 'file cabinet' where all the information objects (files) are labeled and filed properly. Flexible metadata modeling and tagging is what makes the 'file cabinet' a reality.

Information classification, with associated metadata tagging, is the process of identifying information objects. A critical success factor for managing this process, especially in a highly distributed enterprises such as DoD/IC Agencies, is to make the process as transparent and automated as possible. OpenText provides automation tools with flexible methods to make the metadata tagging process efficient and accurate. These methods include Process Based Classification and Automated Classification. Manual classification is the exception rather than the rule: though fully supported, this has proven ineffective in the real world.

Process Based Classification is achieved through interoperability with applications that drive operations processes. As discussed above, integration with front end applications provides operational context and derived metadata, which can be used to automatically 'tag' information objects such as a document attached to a transaction. As tagging is automated, Process Based Classification is transparent to users.

OpenText also provides standards-based Automated Classification capabilities, which analyze and tag information objects across your enterprise systems without programming or migration from source systems. These capabilities are a set of sophisticated content analytics tools, which rely on natural language processing to identify and tag concepts, entities and categories contained within your information. As a part of the analysis process, source system security profiles are also extracted, then correlated with enterprise security context. Thus, a separate security configuration is not required for this capability set.

The result of these combined classification methods is realization of a highly flexible Information Governance and Security solution that is powerful, intuitive and efficient to maintain.

Metadata tagging of information objects related to the investigation is key to management of those objects as evidence. Whether within existing systems or created as part of investigation processes, metadata along with supporting audit logs provide proof of 'chain of custody' of evidence gathered, should charges be brought.

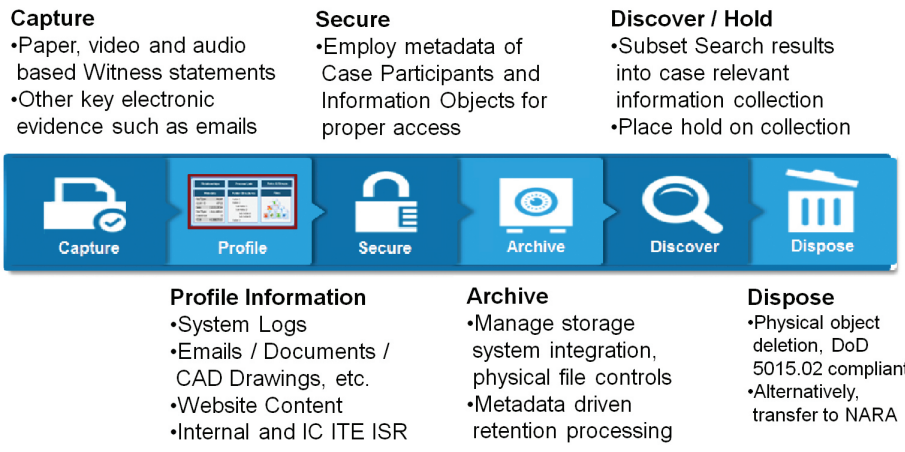


FIGURE 4

Metadata tagging of information objects related to the investigation is key to management of those objects as evidence. Whether within existing systems or created as part of investigation processes, metadata along with supporting audit logs provide proof of 'chain of custody' of evidence gathered, should charges be brought.

Metadata Driven Access Schemas

In every industry, it is imperative to ensure that information access controls meet compliance and governance requirements. A failure to do so can cause a stoppage of operations, financial adjustments, loss of sensitive or secret information, or indefensible evidence in support of investigations and litigation.

Access controls are critical in the creation and management of information across the enterprise. The ability to see results of a search, to read, print, modify or delete content is configurable for each group. Using this approach, content can be made available to only select groups, while other users will not be able to see content within a Search result set for which they are not authorized. Content can be made 'read-only' to a majority of users, allowing only members of select groups to add, modify, or delete content. As prescribed within the DoD 5015.02 / v. 3 standard, supplemental markings metadata may be used to further classify information objects according to DoD information security levels such as 'Controlled Unclassified' (4 and 5) or 'Secret' (6). This applies to data, documents and other content of a sensitive nature.

Security is not just about blocking access, for today's information fueled operations it's also about ensuring the right people have access to the right information at the right time. This applies to information consumers searching for data, navigating folders, following a link from a colleague, or following operational process-flows across systems. Key to an information security schema is figuring out the right balance of access requirements versus security controls. It not as simple a calculation as it may sound. If access is too tightly controlled, an organization runs the risk of hampering mission objectives, innovation and information reuse. If it is too lightly controlled, risk can range from data leakage to tampering, which in turn can jeopardize mission success.

User Role/Group Based Access: For areas such as Accounting, role based access will typically suffice. Example: an Accounts Payable (AP) processor has access to AP transactions in Oracle EBS, and by inference access to applicable attachments/content. Transaction access via EBS may be restricted to a specific command, region and/or cost center, which in turn limits content access. Role based access also includes internal website and email users groups for the AP processor.

Activity Based Access: Investigators and Attorneys involved in a misconduct case will need access to certain (not all) related content, this is 'Activity Based Access'. This must be configured from the case perspective, where access scope is derived from information needed to complete the investigation. Activity based access is additive to the participants underlying role/group access, but does not supersede security clearance constraints. Note, activity based access always expires, this can be time period based or more commonly event based. An 'event' could range from case closure to employee retirement or separation.

Subject Based Access: Whether for an investigation or other operational duties, it is key that Subject Matter Experts have access to information related to their area of expertise, regardless of the domain within which that information resides. Example: this investigation scenario involves Cybersecurity and information exfiltration, so access to relevant technical data is critical for the Investigator. For Attorneys, access to code of conduct, Federal Rules of Civil Procedure, comparable cases and applicable laws is essential. With adequate information profiling via metadata, access to required information for each participant can be configured across solution domains. Note, as with other access methods, this type of access does not supersede information security clearance constraints.

Human resource and training data is needed to gather relevant security clearance, organization / rank, deployment and training information needed to accurately determine access. ERP and other operations support information systems are employed to provide 'virtual metadata' related to mission, program or investigations. Source system metadata is then applied within access authorization schemas.

Leveraging Analytics within Information Governance and Security Operations

IT operations staff are supporting increasingly complex analytics capabilities and growth in information volumes across emerging hybrid infrastructures. Understandably, the focus is on information delivery and analysis solutions in support of mission and business operations. In order to meet the growing demand for complex information solutions in support of DoD/IC mission objectives, it is imperative that IT begins to apply sophisticated analytics to manage information and security.

As mentioned above, content analytics should be employed to profile information, especially 'unstructured' content residing in file shares, SharePoint, email and legacy imaging systems. Through the use of analytics visualizations (dashboards, graphs, etc.), with the ability to 'slice and dice' supporting details, you can begin to comprehensively assess and proactively manage information.

With information profiling in place, OpenText analytics and visualization tools can then be put in place to enable 'Access Analytics.' Access Analytics enables IT staff to understand what information is being used and who is using it, along with process and security context. First and foremost, this will help IT staff to understand the effectiveness of information delivery and analysis systems, capitalize on best practices of effective systems and improve or eliminate ineffective tools. Access Analytics also enables more precise storage management by revealing patterns of seldom accessed information objects that can be moved to cheaper/slower storage.

In addition, Access Analytics is an invaluable solution in information security, where previously undetectable threats, such as exfiltration of related information from multiple systems, can be identified. Information profiles are coupled with analysis of existing user security profiles across all relevant systems to provide a complete view of enterprise level security context.

If a compromise does occur or a suspected compromise is at hand, it is vital to be able to understand the full history of sensitive content and reconstruct its forensic trail. This ranges from who has viewed or downloaded the information to administrative actions such as changing permissions or access within a set of content. Information audit capabilities are a key component of Access Analytics, designed to help you manage and assess threats:

- When and by whom an asset is accessed
- When it is viewed, downloaded or deleted
- When administrative settings or access has changed

Security and Access

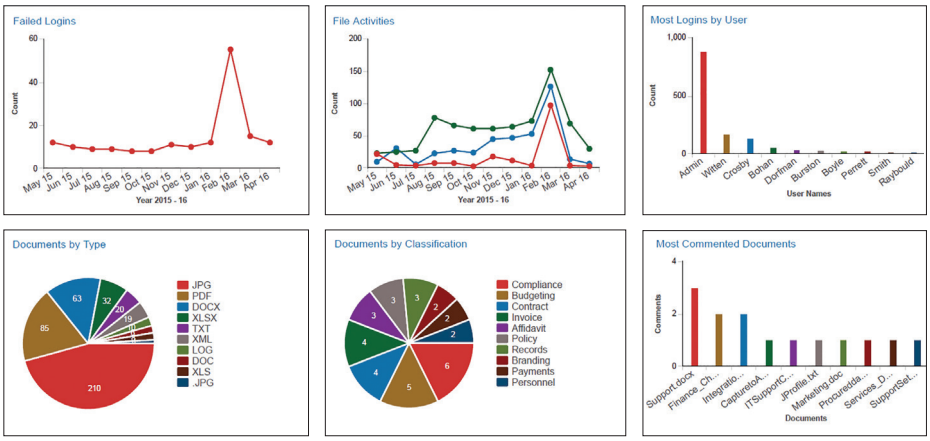


FIGURE 5

- ***Proactively monitor Content access and usage (view, copy, print, download)***
- ***Analyze / respond to vulnerabilities and threats with tools that maintain context of concerns, launch Content Workspace to help manage / document response***

OpenText Analytics enables everyone involved in IT and Cybersecurity operations – not just specialized data scientists – to see data aggregated from multiple sources in visual, easy to digest formats. Personnel can then apply their domain expertise to review operational measures, uncover trends and anomalies in operations and financial reports. OpenText Analytics data visualizations and reports are fully interactive, so users can dynamically: drill down to underlying data, update views or securely link additional data without programming.

Process Governance and EIM

Though often overlooked, Process Governance is a critical aspect of the success of Information Governance and Security solution deployments. When information needs to be retained for litigation or audit support, along with general compliance, it is imperative to ensure that the information remains demonstratively defensible, discoverable and unmodified. Information that is not in this condition via requisite process controls and audit trails can become a threat to the organization. Whether for operations, litigation or audit support, unauthorized access to or damaged information represents a risk to mission success.

OpenText Process Governance capabilities are a cornerstone of the Information Governance and Security solution set outlined herein. Capabilities include a visual modelling and execution environment that allows you to tailor IT operational processes to manage information controls and other agency specific compliance requirements, no matter how simple or complex those processes may be.

Process Governance includes rich capabilities and connectors that allow you to dynamically interoperate with processes and information from your key systems. Key systems supported range from ERP and applications to Cybersecurity, Sourcing and Procurement, CRM/SFA, order management, Maintenance and Repair, and financial management. This enables cross-system process orchestration and monitoring, with underlying reporting and analytics to help drive operational improvements.

As mentioned above, OpenText EIM solutions provide the ability to integrate information via standards based object metadata and related security profiles, regardless of source system. Therefore, role, activity and subject based access can be precisely controlled via front end applications, such as SAP, Oracle EBS, SharePoint or OpenText™ Process Suite.

Where applicable, some controls can be derived from enterprise security solutions, such as LDAP, but those solutions tend toward high level/user group access definition, so are too imprecise for adequate information governance and security control. Legacy systems may also have disparate access management schemas, so may also leave gaps in comprehensive governance strategies. For these systems, Process Governance can bridge the gaps in 'security master data management' through interoperability with those systems, as well as tight integration with EIM metadata and applications described above.

The Process Governance solution set can be enhanced with the OpenText Metrics Manager analytics option that enables an organization to create key performance indicators (KPIs), measure performance against those KPIs, and collaboratively develop

Process Governance Capabilities:

- *Process and entity model design environment*
- *UI elements: Forms, Lists, Layouts, Actions*
- *Analytics, Data and Content integration*

Ad-hoc user-adjustable elements:

- *Milestones, Checklists, Tasks, Reports*
- *Personalization and Localization*

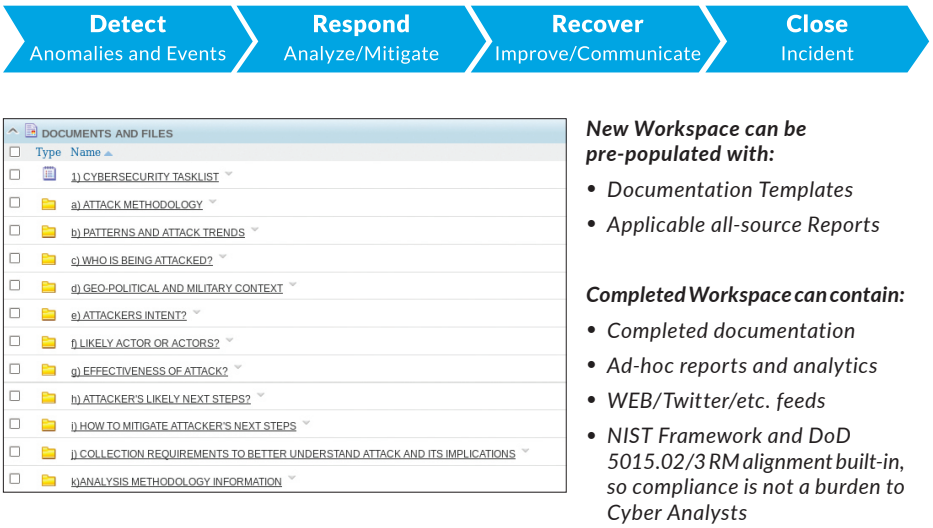
FIGURE 6

Process Governance for the investigation process is critical to consistency and compliance for the information (evidence) captured. Activity Based Access will be assigned at investigation launch, Process Governance can be employed across required systems to ensure proper access is implemented. Throughout the investigation process, access by participants can be limited or removed automatically, based on 'process state' such as investigation close.

corrective action plans to address shortcomings. Aligned with industry standards, these capabilities form the foundation of Governance, Risk and Compliance measures of IT and Cybersecurity Operational effectiveness.

Process Governance for the investigation process is critical to consistency and compliance for the information (evidence) captured. As 'activity based access' will be assigned at investigation launch, Process Governance can be employed across required systems to ensure proper access is implemented. At various points of the investigation, access for specific participant types can be limited or removed automatically, based on 'process state' such as investigation close.

In keeping with the NIST Cybersecurity Risk Management Framework objectives, along with the need to measure and improve overall IT Operations, it is becoming increasingly important to incorporate the standard enterprise Governance, Risk and Compliance (GRC) approach.



New Workspace can be pre-populated with:

- *Documentation Templates*
- *Applicable all-source Reports*

Completed Workspace can contain:

- *Completed documentation*
- *Ad-hoc reports and analytics*
- *WEB/Twitter/etc. feeds*
- *NIST Framework and DoD 5015.02/3 RM alignment built-in, so compliance is not a burden to Cyber Analysts*

POLICY (851001): The cybersecurity requirements for DoD information technologies will be managed... consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 (Reference (c)).

FIGURE 7

As this solution scenario is related to a cybersecurity incident, it is important to note that OpenText provides capabilities in support of cyber-operations. With these solutions in place, case investigator can utilize content (evidence) captured as part of a cybersecurity incident process, greatly reducing time needed to gather key evidence.

Summary of Information Governance and Security Solution Benefits

OpenText EIM provides a comprehensive Information Governance and Security solution set supporting all types of IT systems and related processes across an organization. Solutions meeting DoD/IC specific requirements will be deployed to handle a wide variety of operating models and mission specifications, and can scale to manage extremely high volumes of information. Key solution benefits include:

- **Enterprise Interoperability:** enables a comprehensive governance and security solution.
- **Readiness:** having the means to understand and secure information using real-time profiling and monitoring is a critical step in preventing broad data breaches or damage, whether the threat is from within or without.
- **Information Governance:** the OpenText solution provides multi-layered protection of information, with comprehensive security and governance capabilities.
- **Flexibility:** with the instantaneous changes of the connected age, cybersecurity risks can evolve quickly. In order to effectively respond to rapid risk evolution, OpenText EIM capabilities provide highly flexible solutions that enable IT, SMEs and Operations staff to adjust cybersecurity processes and information capture without coding.
- **Standards based Information Management and Security**
  - Promote situational awareness and collaboration, then provide comprehensive reporting to meet the full range of compliance requirements
  - Alignment with mandated NIST Cybersecurity risk framework and processes
  - Join IT Operations effectiveness measures with enterprise GRC context
  - Provides DoD 5015.02, v.3 Records Management certified capabilities for consistent management of all information, regardless of source
- **Risk Mitigation and Governance capabilities enable an enterprise level solution**
  - Quickly locate then secure PII/Secret/Top Secret information with automated Content Analytics, limiting risk without costly programming, customized integrations or lengthy migrations
  - Supplier certified embedding of EIM capabilities within SAP, Oracle EBS, and SharePoint, along with COTS integration, enables consistent security
- **Information usage pattern analysis:** information that is frequently accessed is maintained on the highest speed infrastructure, whereas information seldom accessed can be automatically moved to slower/cheaper storage. As agencies move to cloud based infrastructures, effectively managing information asset location can help generate significant cost savings.

OpenText EIM solutions enable improved operations, while meeting process and information governance requirements without placing additional burdens on IT operation analysts or oversight staff. The solution is COTS based, so near term implementation and adoption, along with long term support costs are lower.

About OpenText

OpenText enables the digital world, creating a better way for organizations to work with information, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTC) visit opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn | Facebook

www.opentext.com/contact