P. O. Box 1407
Garner, NC 27529

November 2011

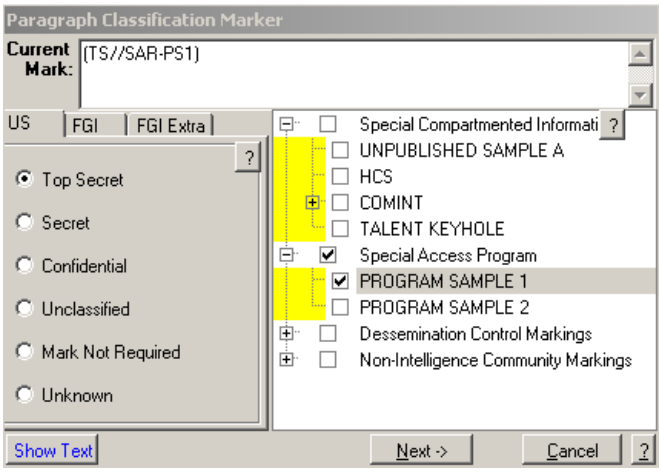
The WIKILEAKS debacle was preventable! Do not let it happen on your watch to your organization!

Digitaltide's patented solution addresses seven critical, and systemic information security problems in an electronic information environment:

- Inconsistent and inappropriate information/document classification and classification mark determinations;
- Paper based classification regimes;
- Lack of oversight of document/file access, movement, derivation, classification and declassification;
- Inability to identify and resolve potential "Insider Threats" whether inadvertent or intentional;
- Manual declassification;
- Trade-off of "need-to-know" access policy for the productivity of electronic information systems; and
- Imprecise user activity documentation.

Digitaltide addresses these as well as other information security needs by means of common-sense solutions that do not downgrade the productivity gains organizations have achieved by means of electronic information networks and the productivity attributes of document development software applications.

Document Classification:



<u>You can't effectively control valuable information unless you know the value!</u>

Digitaltide focuses first on the classification of information/documents by presenting users of document development software applications with an easy to use, portion by portion, classification and marking tool with immediate access to classification guides and other guidance. The tool works in harmony with a documet development application and provides a point and click classification environment for the user/classifier that generates an overall document classification mark based on user portion classification determinations. Each user classification tool is dynamically configured for the security clearance and access level authorized for each user. Documents are not static in an electronic environment and the classification mark generated changes as the information in the document is changed by users. Digitaltide's Classification Marker Suite (CM-Suite) provides immediate and persistent classification mark feed-back to users on both the information in an output view of the electronic document/file, that may be a subset of information contained in the document/file, as well as the entire informational content contained in the electronic file. These two separate classification mark determinations are automatically generated and displayed to the user/classifier within the document development application. Classification determinations and marks that may differ and require different handling and protection depending, for example, whether the electronic file is being moved or shared on the system or the output subset, is being displayed or printed.

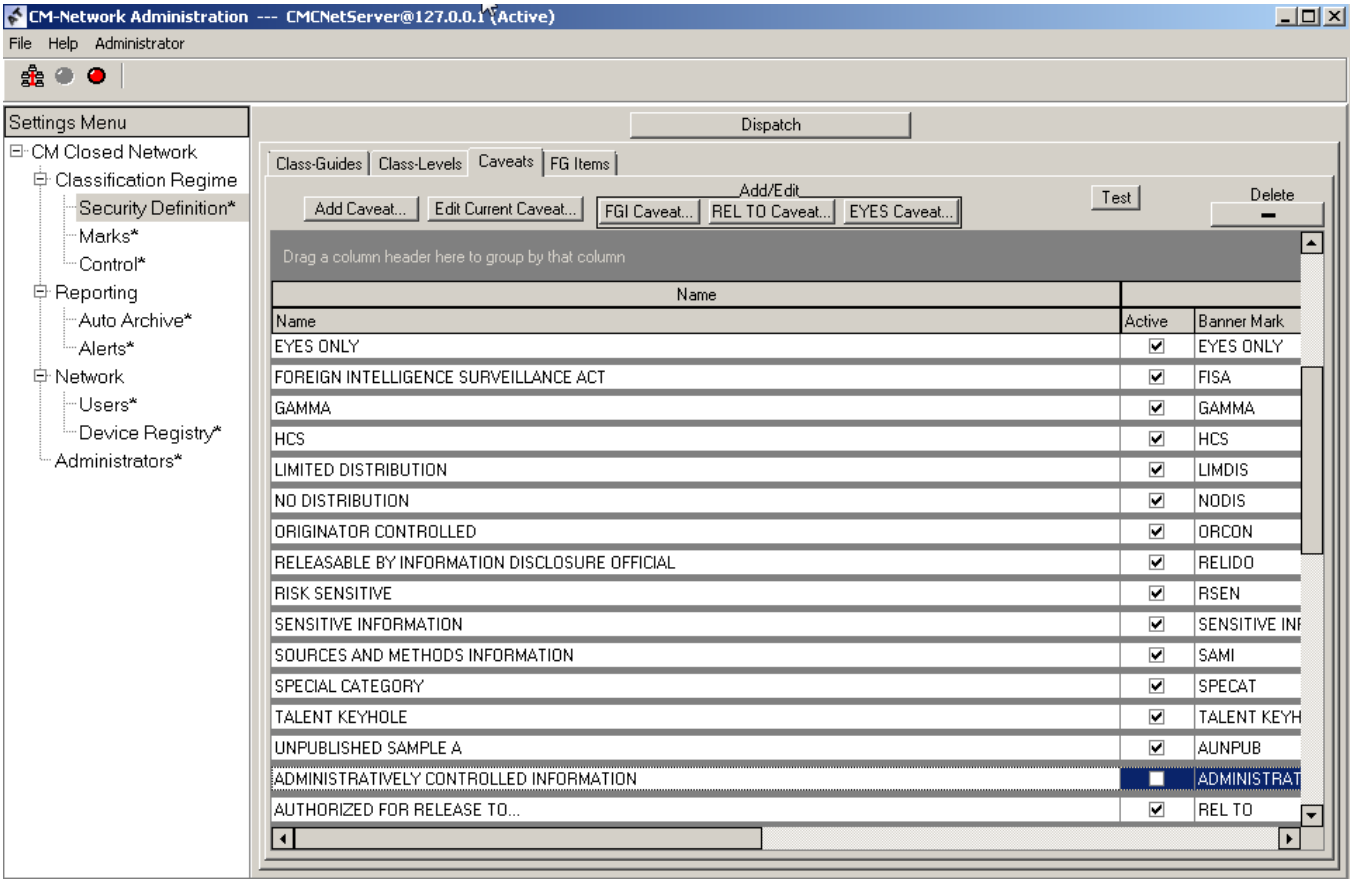
The tool automatically generates an interim classification mark with a "system high" classification designation for documents/files that are working documents, incomplete documents or documents in draft mode assuring that every document is marked and that system users can differential between unclassified documents that may require no classification marks in the document output and documents that have not yet completed the classification process. Additionally, Digitaltide's CM-Suite provides exceptional audit trails to assure that individual users can be held accountable for their classification determinations and their operations on electronic documents.

The Digitaltide classification tool simplifies the complexities of user document classification and marking training and handles legacy documents preexisting on a system or network. However, the tool does not lock users into a classification structure that may not meet the classification need for an occasional, anomalous document classification requirement. Users may opt-out of the classification tool to mark a document manually, however each such action is documented and logged, and the user must provide a reason for the action and he or she is required to certify the final classification of the opted-

out document. Opting-out of the marking tool does not remove the document from Digitaltide's rigorous monitoring and oversight capability.

.

Flexible Classification Regime:



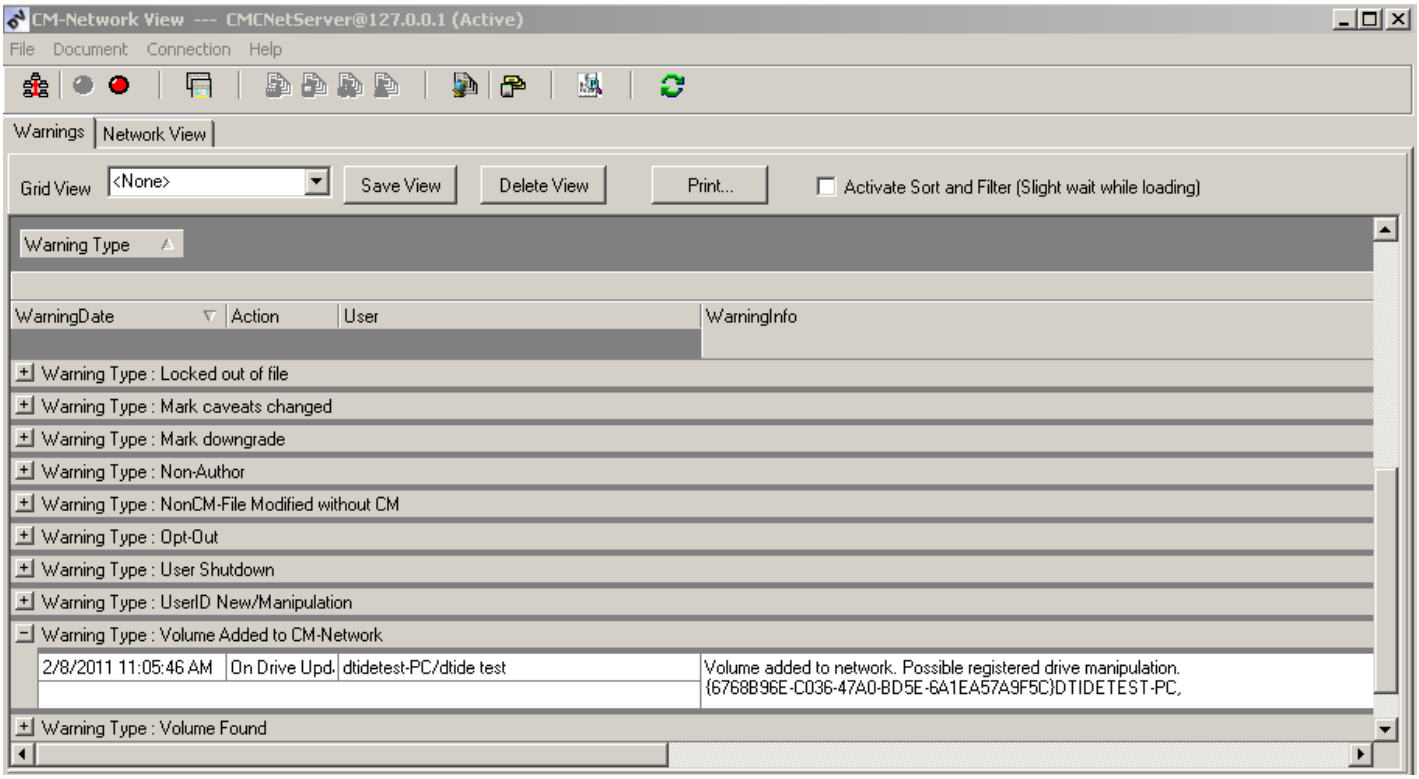
The complexity and requirements of the U. S. classification and marking system for national security and sensitive information are difficult to implement and little understood outside of information security specialists and the Intelligence Community!

In order to accomplish reliable national security classification determinations Digitaltide has developed a network-wide or domain-wide controlling classification regime structure. The regime's administrative tool enables in-house personnel to establish the structure and classification requirements for the organization. It is not necessary to brief new personnel thereby providing the keys to the kingdom to establish and maintain a regime. The regime is pre-loaded with the "open" elements of the Controlled Access Program Coordination Office (CAPCO) classification structure. However tools and dialogs enable administrators to add Special Access Program designations, Sensitive Compartmented Information compartments and sub-compartments, or handling instructions or otherwise modify the CAPCO regime to meet the unique classification environment of a system, network or organization, as well as establish the organization's mark format requirements. Tools within the classification regime's administrative tool allow administrators to test changes to the classification regime before those changes

are disseminated across a network

The Classification Regime administrative tool enables an administrator to establish the format and location of document classification marks generated by the system and to set user "classification profiles" in support of multi-level system classification environments. The regime automatically establishes a unique coding system as the classification regime is established or modified. The coding structure enables the user classification tool to uniquely code and embed in a persistent manner the document/file classification determinations into the electronic file, separate and apart from the classification marks generated for the informational content of the file. It is critical to oversight of classified information on electronic systems/networks to know the classification value of a document at all times as well as the classification value of all information stored on an electronic storage media devices. Digitaltide's oversight process maintains the document's classification value even if an "Insider " should remove classification marks or remove the corresponding embedded codes from a document by unauthorized means outside of the Digitaltide process. Such user activity is logged and generates an immediate security warning.

Oversight:



<u>Classification and marking documents on electronic systems is relatively meaningless to an insider determined to compromise information unless the marks are persistent, and user document activity is registered and logged!</u>

By means of the persistent classification values coded and embedded into an electronic file, the Digitaltide system provides a positive means and the tools for System Security Administrators (SSA)

to monitor and oversee user document/information activity. The Digitaltide solution records user access to and movement of documents on the system, changes to the document's classification and/ or informational content, copy and paste activity, new documents derived from existing documents, as well as many other user initiated or operating system initiated actions involving electronic documents/ files and the electronic storage media on which they reside. In addition to receiving automated warnings of potential insecure activities generated by the Digitaltide system, SSA's are able to display, arrange, and analyze the data logged for user behavioural analysis and classification system security oversight purposes.

Insider Threat:

The damage can be the same whether or not a compromise was inadvertent or intentional!

The Digitaltide real-time monitoring capability enables SSA's to select pre-configured user activities or system events that may be indicative of an insider threat or otherwise meaningful about the security of information on their systems, and to establish and direct automated e-mail alerts. The alerts provide the basis for an immediate response to resolve highly likely insecure activity. Quick administrative action can avoid costly and lengthy damage assessment investigations and system purge activities. Inadvertent compromise of classified or sensitive information can be as damaging to national security as intentional compromise. It is much preferable to meet a culprit at the exit of your secure facility rather than reading about your sensitive or classified information on-line!

The underlying patented technology that drives assisted classification and monitoring functions also provides a platform to establish virtual security perimeters without compromising classified or sensitive elements of a classification regime on open networks. The productivity demands of the information explosion require multi-level classified systems operating side by side with open systems in secure facilities. Digitaltide's perimeter system provides security procedure assurance by providing e-mail alerts to security personnel should unauthorized movement of classified information to an open system or a lower classified system occur and provide a basis for immediate automated counter-measures on the receiving computer as well as a security personnel response.

Declassification Support:

Effective declassification is pro-active declassification!

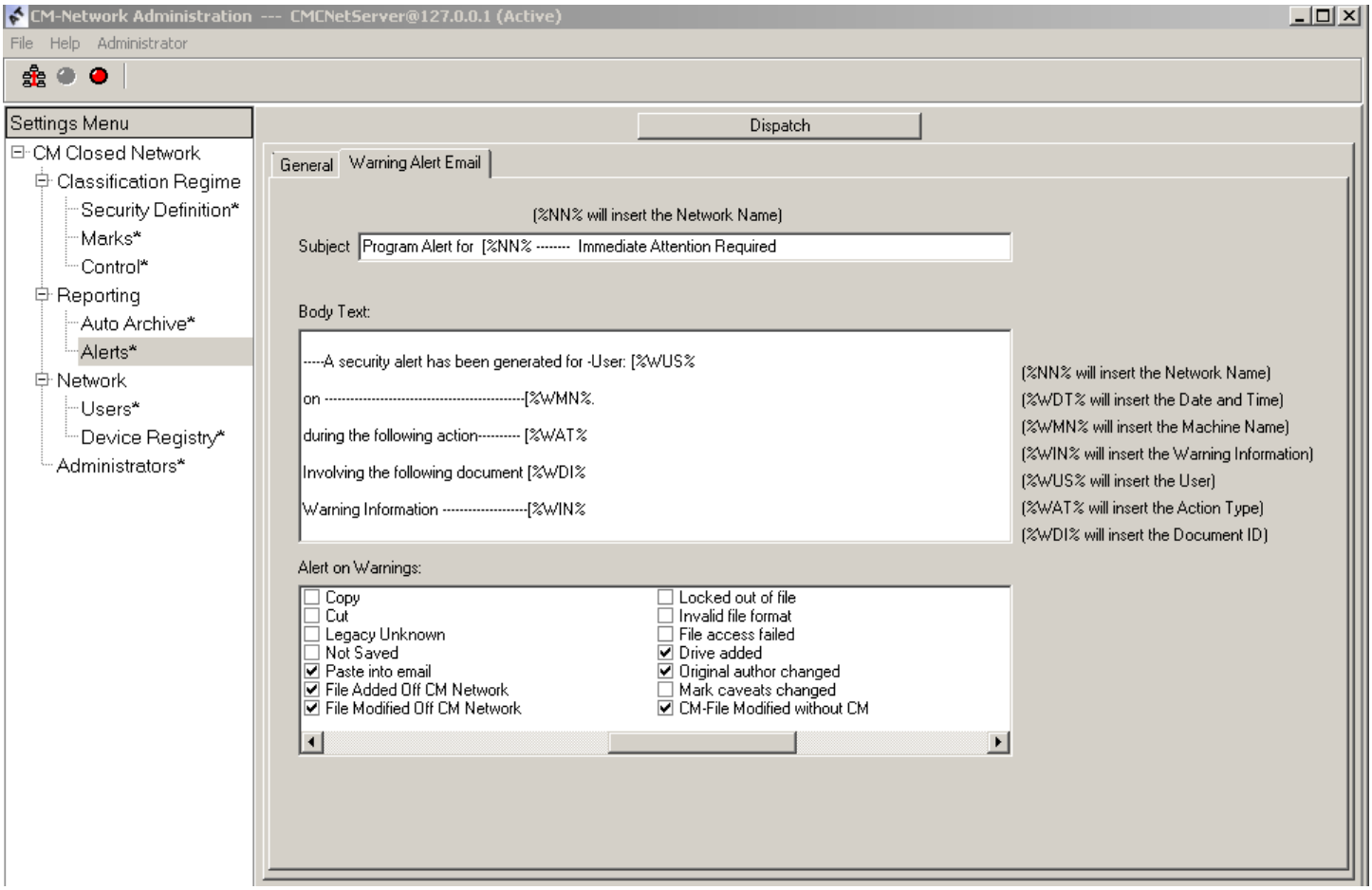
As a result of the Digitaltide methods, electronic documents can be identified and located on any of a document's classification mark criteria, either portion marks or overall classification marks, as well as any of the classification block criteria required in the Digitaltide system to maintain a final document classification for national security information. This includes de-classification information. The Digitaltide system enables system administrators to pro-actively identify and locate documents requiring de-classification in accordance with national declassification policy. The classification block information is an integral part of the Digitaltide classification solution. The classification block information is also captured, logged and monitored and the information is also coded and embedded in each electronic file. The Digitaltide tools enable SSA's to identify and locate documents/files across a network, or across network domains, on any classification or declassification criterion.

Need-to-Know

Risk of compromise of national security information increases by the number of individuals who are aware of the information!

Organizations mitigated the strong "need-to-know" policies of the nation's paper-based national security classification management system for the productivity of electronic systems when integrating classified information into electronic systems. The trade-off enables users of electronic systems to peruse documents/information within the system and provides access to an exponentially greater amount of information than would have been available to a user in the paper-based system controlled by a need-to-know policy. Digitaltide's document monitoring system enables security administrators to identify a user's pattern of document access that may be indicative of unnecessary and/or unauthorised access to classified information.

Support for Enhanced Investigative Tehniques



To initiate a security or counterintelligence investigation a potential problem must first be identified!

Digitaltide's rigorous document monitoring and user activity oversight capability coupled with automated warnings of potential insecure user activities enables a new level of security/ counterintelligence capability for national security protected networks. Not only does Digitaltide provide the means to identify a potential "Insider Threat" problem, but the patented monitoring matrix that

uniquely codes and associates documents with document storage media, document storage media with computers on the network, and computers to the network itself, provides a new level of confidence in the activity logs generated by CM-Suite. Digitaltide is confident that logs documenting user activity on a network will support the evidentiary requirements for a request to authorize enhanced investigative techniques under the Foreign Intelligence Surveillance Act (FISA).

Digitaltide's unique platform that persistently codes document classification values, and monitors document activity provides other potentially sensitive security and counterintelligence methods that are not appropriate for disclosure in this document.

For more information please visit our webpage at http.www.dtide.com or call (202) 747-0041.