RFI Questions and Government Response

Q1. What is the format the contents are in? Are these structured formats such as comma separated values (CSV), extensible markup language (XML) or are they binary or proprietary formats such as PDF?

A1: Protection of any file type on a Microsoft operating system (OS) file system and active directory domain would be ideal. In particular stakeholders would like the capability to label audio and video files.

Q2. What are the means of access to the information that DoD seeks to restrict? Is the access Web Based (HTTP), other protocols such as simple file transfer protocol (SFTP)?

A2: The primary mechanism for user interaction and secure communication is via software collaboration tools versus use of specific network PPS. If the software protects files at the OS level, that information should automatically update any attachment of the files to the collaboration software. But, at a minimum the software must work with Microsoft Office products, including outlook / exchange, SharePoint, and Lync.

Q3. Please elaborate on the type of tool you envision. Is this intended as a manual or automated capability? How is information intended to be marked (i.e. XML Meta Data, Digital Signatures, etc.)?

A3: The tool should be predominantly automated, with privileged users (ie ISSMs, ISSOs, or maybe even GSSO) should be able to manually override the automation of the tool. Which in essence means the software must have role-based privileges capability.

The tool should assist the user by preventing marking mistakes and inadvertent disclosure/sharing. The tool will require the user to ultimately define a security classification marking but might offer suggestions based upon dirty words or internal classification markings. The tool will perform all enforcement functions to prevent unauthorized access. The tool may assist the user with internal document markings on human readable files (e.g., Microsoft Word Document) but must also apply security attributes to non-human readable formats (e.g., binary and machine data) so that the system can adjudicate access. The tool shall provide audit of user actions (initial marking, where, when, upgrades, downgrades, etc.) that can be consolidated into a Security Incident and Event Management (SIEM) system. Markings used for access adjudication shall be available to the user much like other file metadata (e.g., file name, file size, date modified, etc.)

XML – eXentisble Markup Language
CSV – Comma Separated Value
PDF – is a file extension, not sure if it is an acronym for something
MSFT – Microsoft
OS – Operating System
CV2 – Combat Air Forces Network Version 2
HTTP – HyperText Trandfer Protocol
SFTP – Simple File Transfer Protocol
PPS – Ports, Protocols, and Sevices

ISSM/ISSO – Information System Security Manager/Officer
GSSO – Government SAP Security Officer