Mapping Between
Application Software Extended Package for Redaction Tools, Version 2.0, 2015-12-11
and
NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System**. The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context.** Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **MP-6 and AC-4(23)**. The primary purpose of a redaction tool is to search digital content for sensitive data that may be subject to sanitization. A redaction tool is therefore intended to support an organization's implementation of MP-6. If the redaction tool is deployed in such a way that digital materials are scanned when transferring information between security domains, AC-(23) would apply as well, though a redaction tool may not necessarily support this capability. Assessors must be aware of the intended usage of the redaction tool to understand the security controls it is intended to satisfy as a whole.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to redact data only supports MP-6 to the extent that the organization requires redaction of certain sensitive data from documents. It would not address other aspects of MP-6 such as the secure disposal of physical storage devices as part of the decommissioning of some part of the system. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported.

Common Criteria Version 3.x SFR		**NIST SP 800-53 Revision 5 Control Supports**		**Comments and Observations**
TOE Security Functional Requirements				
REP_GEN_EXT.1	**Report Generation**	AU-12	**Audit Generation**	A conformant TOE supports this control by generating a report of its usage.
REP_RVW_EXT.1	**Report Review**	AU-6	**Audit Record Review, Analysis, and Reporting**	A conformant TOE supports part (a) of this control by providing a mechanism to

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				review reports of system activity.
VAL_REM_EXT.1	**Validation of Data**	MP-6	**Media Sanitization**	A conformant TOE supports this control by applying its redaction functionality to extraneous data from source materials since that data may be used as a hidden source of sensitive material.
RED_SEL_EXT.1	**Selected Redaction**	MP-6	**Media Sanitization**	A conformant TOE supports this control by applying its redaction functionality to embedded and graphical objects.
RED_DIN_EXT.1	**Deep Inspection**	MP-6	**Media Sanitization**	A conformant TOE supports this control by applying its redaction functionality to metadata and nested objects.
RED_RPL_EXT.1	**Visible Space Replace**	MP-6	**Media Sanitization**	A conformant TOE supports this control by performing redaction in such a manner that the redacted data does not give any clues as to the original data.
RED_REM_EXT.1	**Removal of Redacted Data**	MP-6	**Media Sanitization**	A conformant TOE supports this control by redacting the data that is marked by the user for redaction.
RED_LOC_EXT.1	**Redact Content from Every Location**	MP-6	**Media Sanitization**	A conformant TOE supports this control by redacting all instances of the data that is selected for redaction.
RED_NND_EXT.1	**No New Data Introduced by TOE**	N/A	**N/A**	This requirement is for the TOE to avoid adding data or metadata to a file that is being redacted. There are no security controls that relate to this behavior.
RED_OBJ_EXT.1	**Removal of Objects and Corresponding References**	MP-6	**Media Sanitization**	A conformant TOE supports this control by removing all references to redacted data.
RED_RIP_EXT.1	**Residual Information Removal**	SC-4	**Information in Shared System Resources**	A conformant TOE supports this control by ensuring that residual data is erased from temporary storage so that unredacted data cannot be read by another

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				process that accesses this storage.
FPT_FLS.1	**Failure with Preservation of Secure State**	SC-24	**Fail in Known State**	A conformant TOE supports this control by failing in a known state, which in this case is a state where the TOE does not output an unredacted or partially redacted file when a failure occurs.
RED_ID_EXT.1	**Identification of Data**	MP-6	**Media Sanitization**	A conformant TOE supports this control by giving the user an interface to select the data that will be redacted from the input file.
RED_RVW_EXT.1	**Element Review**	MP-6	**Media Sanitization**	A conformant TOE supports this control by giving the user an interface to select the data that will be redacted from the input file.
RED_ALR_EXT.1	**Redaction Failure Notification**	SI-4	**Information System Monitoring**	A conformant TOE supports this control by generating an alert in response to a failure of the TOE’s operation.
Optional Requirements				
No optional requirements defined.				
Selection-Based Requirements				
No selection-based requirements defined.				
Objective Requirements				
No objective requirements defined.				