File 20090126.2116: I wrote a long paragraph about NSTISSP № 11 for Kevin Miller: reproduced below:

> NSTISSP № 11 requires that preference be given to evaluated or validated products to be used for national security processing ('national security' is defined in NSD 42). This means in practice a Common Criteria certificate—in the case of products evaluated at EAL4 or below by any of the thirteen certificate-authorising countries, or specifically a NIAP CCEVS issued certificate for products evaluated at EAL5 and above; or a FIPS 140-2 validation in the case of cryptographic modules. RM incorporates a FIPS 140-2 validated cryptographic module when we link to the particular OpenSSL version that we use. However, the FIPS 140-2 validation applies to the OpenSSL component only, not to the entire RM system. RM is not Common Criteria evaluated. This is primarily because RM is a GOTS IA-enabled product dating from before the effective date of the policy; secondly because of the close development and testing relationship RM has always had with the Information Assurance Directorate (IAD) of NSA; and finally because RM was developed specifically under DCID 6/3 rules, not NSTISSP № 11. Note that this is not the same as a Deferred Compliance Authorization (DCA); there is no DCA specifically addressing RM (any DCA would only be for a specific acquisition anyway). The developer and the RM Programme Office consider that the circumstances surrounding the development of RM were different from what is addressed by NSTISSP № 11 (more stringent than NSTISSP № 11) and that therefore NSTISSP № 11 does not affect RM.
>
> IA has always been treated as a requirement in the development of RM.

References