Guidance from the
National Information Assurance Partnership
21 October 2014

Usage of the Protection Profile for Application Software

The requirements in the *Protection Profile for Application Software* apply to mobile applications (*apps*), as well as application software on desktop and server platforms.

However, this broad scope does not imply a Common Criteria (ISO/IEC 15408) evaluation is realistic or required for such a vast number of commercial software products. Instead, the position of NIAP is that:

- The Protection Profile (or more-specific Profiles) is to be used for Common Criteria evaluations of IA and IA–enabled products on US National Security Systems as required by CNSSP #11. Vendors seeking a CC certificate must be evaluated according to the Common Criteria Recognition Arrangement (i.e., by an accredited CC test lab within a CCRA scheme).
- The Protection Profile is suitable for use as a baseline set of security requirements by organizations engaged in evaluating (often called *vetting*) mobile apps, as well as desktop and server applications, outside the formal Common Criteria. This includes government agencies as well as commercial app stores. Although such evaluations cannot be awarded a formal Common Criteria certificate, the PP provides a sensible baseline for their evaluation activities. An alternate representation of the Protection Profile, entitled *Requirements for Vetting Mobile Apps from the Protection Profile for Application Software* is provided explicitly for this purpose. These requirements also provide a basis for decision-making by Authorizing Officials who must weigh risks and then decide between using commercial app stores and investing in government-run app vetting services.
- The Protection Profile complements NIST Special Publication 800-163, *Technical Considerations for Vetting 3rd Party Mobile Applications*, available at http://csrc.nist.gov. The Special Publication provides key technical considerations for organizations as they adopt mobile app vetting processes within the larger context of their enterprise information systems. It includes security and non-security considerations (such as accessibility and performance), and also describes characteristics of tools which can be used to automate vetting.

The Protection Profile serves a diverse set of stakeholders within government, and allows for the coordination of a single set of requirements with industry. The NIAP Technical Community for Application Software will continue to evolve the document, and participation remains open to government, industry, and academia. The Protection Profile also provides a body of base requirements for the development of many Extended Packages for more-specialized types of software.