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 Protection Profile is to be used for Common Criteria evaluations of IA and IA–enabled products. Vendors seeking a CC certificate must be evaluated according to the Common Criteria Recognition Arrangement.
- CNSSP #11 mandates that IA and IA-enabled COTS products for use on US National Security Systems be evaluated against a NIAP approved PP. For IA and IA-enabled software applications, evaluation against the *Protection Profile for Application Software* is required for compliance with CNSSP #11, available at https://www.cnss.gov.
- The Protection Profile (PP) is suitable for use as a baseline, consistent set of security requirements by organizations engaged in evaluating ("vetting") mobile apps outside the formal Common Criteria. This includes government agencies as well as commercial app stores. An alternate representation of the PP, entitled *Requirements for Vetting Mobile Apps from the Protection Profile for Application Software* is provided explicitly for this purpose. Although such application vetting cannot be awarded a formal CC certificate, the PP provides a sensible baseline for app vetting activities.
- The PP allows for a consistent set of requirements for use by the makers of app vetting tools. App vetting is only practical when highly automated, and so use of automated tools is key. Formal Common Criteria evaluations will also enjoy a reduction in both cost and time when automated tools are applied.
- The PP provides a basis for decision-making by Authorizing Officials who must weigh risks and then decide between using commercial app stores and investing in government-funded 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. NIAP and the International 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 or Modules for more specialized types of software.