SKPP Sunset Q&A

1. What is happening to the SKPP?

- NIAP will sunset the SKPP.
- IAD will focus on specific Government systems using Separation Kernels rather than general OS evaluation and assurance maintenance.

2. How does NSA plan to address EAL 5 and above? What role will formal methods play?

- NIAP will focus on the lower EALs. These are applicable to generic commercial products.

- For EAL 5 and above, the details of a good security argument are very specific to the system and environment. The issues with SKPP assurance maintenance on commodity desktops exemplify this. As a result, when such systems are necessary, NSA will focus on Certification and Accreditation (C&A) for the specific Government systems.

    - "Security" is not just about meeting requirements. It requires continuing effort, even after the "requirements" are met. This is not captured well by an EAL. The expectation is that a higher EAL is "better" and can simply be trusted to a greater degree in any system built. Unfortunately, the actual evidence that supported passing the EAL requirements does not necessarily support the system's environment, configuration, and use case. This is especially true as operational requirements force implementation changes such as updates, newer hardware, and different configurations. In order to support the US Government, NSA will focus its limited resources on arguments and evidence for specific Government systems when High Assurance is required.

- The role of formal methods is to provide convincing evidence. However, they are costly and usually not enough by themselves. Therefore, most systems do not use formal methods. They may still be useful for systems that need to make very specific arguments, though.

3. Does NSA still support investment in Separation Kernel development/use? Should I continue to refer to the SKPP when building a separation kernel?

- Yes. Separation Kernels, and the Least Privilege architecture that they support, continue to be sound design choices for security-critical systems.

- NSA will not, however, continue to support certification of operating systems (including Separation Kernels) in general. Requirements from the SKPP or other PPs may be reused in the context of Government programs seeking to obtain evidence. Still, the focus will be on the assurance argument and evidence for a system, rather than passing/failing requirements. Also, the whole context of the system must be considered, not just the kernel.

4. When and where is High Assurance appropriate?

- All security-critical systems (including those that were initially developed for High Robustness, such as Separation Kernels evaluated against the SKPP) must continue improving their assurance arguments by collecting evidence.

- High Robustness was intended to address systems exposed to an attacker with high attack potential. Essentially, it aims to address the *most difficult* threat environment by requiring the *most rigorous and convincing* assurance evidence possible. In general, this still makes sense. High Assurance (e.g. evidence from formal methods, such as that which would be required for EAL >= 5 or High Robustness) is appropriate when attempting to make a convincing security argument in a situation where great skepticism is expected.

    - However, even High Assurance evidence may not be sufficiently convincing for some systems. Even the best assurance evidence possible does not justify some risks. This issue must be thoroughly examined in the context of the Government C&A process.

5. What is changing with regard to NIAP evaluation and support to government programs like Cross Domain Solutions (CDS), especially regarding operating systems?

- NIAP is focusing on the common case of commodity systems solving basic security problems. Therefore, NIAP will issue PPs at EAL 1 and 2. It will not address the specific needs of Government systems that require higher levels of assurance.

- For critical Government systems, the IAD will work within the existing C&A processes to provide the assurance evidence that is available and give guidance regarding the improvement of such assurance evidence. IAD's limited analysis resources will need to be managed to both make concrete and rapid progress where critical needs exist and strategically incorporate improved assurance arguments into a multitude of systems and environments. This will take time.

    - As assurance evidence is collected for numerous Government systems, IAD may revisit the idea of collecting functional and assurance requirements into a PP.

6. How do I engage NSA early on to ensure successful evaluation?

- U.S. Government customers can begin engaging with NSA through client advocates. Many programs already have ISSE support. As specialized vulnerability analysis becomes necessary additional NSA resources may become involved.

7. What is the difference between High Assurance and High Robustness?

- The term *High Robustness* is an indication of confidence in a system such that it can be relied upon to enforce security policy even when exposed to a very capable attacker. The term *High Assurance* is an indication of very convincing evidence that a system has a given set of properties. One would use High Assurance evidence to create a High Robustness system.

8. Without the SKPP, how will we differentiate High Robustness kernels?

- High Robustness must be considered relative to a specific system and its threat environment. If a kernel successfully supported security arguments such that it was appropriate for a High Robustness system (and if its use in that system is public knowledge), this can be used to distinguish those kernels (or other components).

- In addition, assurance evidence for components like a kernel should become more transparent, as NSA implements new evaluation processes. This will be especially useful to government customers, who may be able to reuse evidence or the procedures for collecting it.

9. Will NSA support assurance maintenance? How will upgrades/patches be handled?

- For separation kernels already in evaluation against the SKPP, 2 years of assurance maintenance will be accepted through NIAP. Only minor changes to the original TOE will be allowed. During the next 2 years, IAD will transition support for Government systems using separation kernels away from assurance maintenance through NIAP and directly support the operational security requirements of specific systems.

- For government systems, maintenance is regulated by the Certification and Accreditation process. However, new NSA processes and community involvement are expected to focus these efforts on leveraging program milestones for timely implementation of additional security improvements, including upgrades and patching. Collaboration with the security community both inside and outside the US Government will be necessary to realize this goal.