**Phase 1: Security (SEC):**

Introduction: SEC phase is the first phase that occurs in the PI architecture and has responsibilities like managing restart events, creating temporary memory, validating root of trust and finally pass hand off information to PEI phase.

Responsibilities:

1. Handling all platform restart events:
   1. Applying power to the system from an unpowered state
   2. Restarting the system from an active state
   3. Receiving various exception conditions
   4. SEC phase can pass optional information to the PEI foundation, such as health information of the processor
2. Creating a temporary memory store: Processor cache will be programmed to behave as linear memory. This cache behavior is called “No Eviction Mode”.
3. Serving as the Root of Trust in the system: SEC phase is the initial code that take control of the system. It authenticates the PEI foundation from the SEC phase before invoking the PEI foundation.
4. Passing hand off information to the PEI foundation: Final responsibility of SEC phase is to pass the following information filled in EFI\_SEC\_PEI\_HAND\_OFF structure to PEI.
   1. State of the platform
   2. Location and size of the Boot Firmware Volume (BFV)
   3. Location and size of the temporary RAM
   4. Location and size of the stack
   5. Optionally, one or HOBs via EFI\_SEC\_HOB\_DATA\_PPI. The HOB structure is passed as arguments to the PEI foundation entry point.

SEC Platform Information PPI: Handoff information is passed from SEC phase to the PEI foundation using the EFI\_SEC\_PEI\_HAND\_OFF structure and list of PPI descriptors is passed to PEI entry point. One of these PPI’s is EFI\_SEC\_PLATFORM\_INFORMATION\_PPI.

SEC HOB Data PPI: SEC phase HOB data is passed to PEI or DXE consumers using HOBs. If EFI\_SEC\_HOB\_DATA\_PPI is in the list of PPIs passed to the PEI entry point, the PEI foundation will call GetHobs() member function and installed all HOBs returned into the HOB list.