Laptop and Technology

Q1: Please explain the process for procuring laptops for the agency?
A1: An Agency organization identifies a business need for laptops. Organization prepares a shopping cart via SCEIS SRM describing in detail items and quantities required and appropriate funding source. Shopping cart is routed electronically for appropriate approvals. Approved shopping cart is routed to Procurement for processing. Procurement procures laptops through existing statewide term contracts for **PCs, Servers, Storage, Peripherals (printers)** established by the State Fiscal Accountability Authority.

Q2: Who is responsible for updating the laptops?
A2: For hardware updates, each Agency organization is responsible for defining the business requirements and funding for new hardware purchases. Hardware vendors are responsible for hardware repairs per any warranty or maintenance agreements.
For software updates, an Agency organization may procure specialized Commercial Off-the-Shelf software. In these cases, the software vendor is responsible for updates per license and maintenance agreements. Office of Information Technology (OIT) also provides updates for specific internally written software, operating system and security updates where required or as requested by the Agency.
SCDPS employees are responsible for connecting to the SCDPS network as required to receive security updates.

Q3: How is this information tracked in SCEIS?
A3: Purchases are tracked in SCEIS. Once a device is received by SCDPS, Records Management enters the asset information into SCEIS. Transfers of ownership are tracked internally via paper forms with signatures required and also recorded in SCEIS.

Q4: Please describe the process utilized by the agency to ensure that when new laptops are issued to troopers, the laptops are fully functional.
A4: Once a laptop is received, tagged, and the owner identified, the Office of Information Technology (OIT) installs required software including internally written applications, purchased products, and required security products. Testing is performed to ensure operability.
For efficiency and standardization, when large quantity purchases are made (as in the case of a graduating class), OIT prepares and tests one "image" for duplication to multiple devices. This process may not provide the ability to configure some software and "in vehicle" settings.
When significant hardware or software changes/additions are necessary, OIT "pilots" a configuration with a small set of users to identify issues prior to release.

Q5: Of the new laptops issued to the 62 troopers that recently graduated from the law enforcement academy, were none of them in proper working condition? If so, why and what has been done to avoid a situation like this occurring in the future?
A5: The 62 laptops were utilized during Training prior to graduation. Once the troopers received their assigned vehicles and connected the laptops to the vehicle docking stations, printers, and scanners, three significant issues were reported:

- the GPS was not functional via the ReportBeam Software(Commercial Off-the-Shelf product)
- "in vehicle" printer issues
- "in-car" video playback feature was not functional

OIT implemented corrective actions for the reported issues and recommended corrective actions to improve the process:

1. Providing an "in vehicle" configuration appointment for the Trooper upon receipt of their assigned vehicle to ensure that the laptop is functioning properly with the "in vehicle" equipment.

2. Working with commercial software vendors to better coordinate changes across products to maintain compatibility.

3. Extending the testing period and increasing the number of "in field" participants.

Q6: The Department of Administration has a Division of Technology which offers a wide variety of information technology products and services to state agencies. Does DPS take advantage of any of the products and services available from the Department of Administration to ensure DPS's IT department, laptops, and other technology are operating at full force and with proper backups?
A6: SCDPS has partnered with the Department of Administration's Division of Technology Operations team and meets regularly with our Account Representative to define and implement solutions. SCDPS currently utilizes DTO's solution offerings for two-factor authentication (SafeNet), third-party patch management (Flexera), and whole disk encryption services (Symantec). SCDPS is currently working with DTO to migrate to McAfee. DTO provides security monitoring for SCDPS' networks to identify viruses, malware, phishing, and other events. SCDPS works with DTO for threat detection. SCDPS recently toured the DTO data center and is awaiting their CJIS/NCIC certification. SCDPS is currently working with Excipio and DTO for Disaster Recovery Planning.