Project Description and Outcome

First responders need trustworthy devices that protect their information and activities when assuming different roles. In non-crisis contexts, such devices could separate normal activities from those requiring transient trust, e.g., banking, health care and personal data management. But, during an emergency, the first responder may be need to access data owned by other government agencies or even by private parties. They may sometimes be required to temporarily access highly classified information. Such information sharing is possible when the data providers are able to control how and when their information can be used.

New software separation kernel technologies, when coupled with hardware extensions for security, can be enhanced with communications and functional support that provides an essential building block for the secure management of local and/or remote information in multiple contexts. The SecureCore project combines advanced research in hardware and software security architectures, protected communications, and mobile device security, while broadening educational opportunities in these areas.

The SecureCore architecture is fundamentally different from existing systems as it enables transient trust and controlled sharing of critical information, which is absolutely required by first responders who must address emergent threats and attack scenarios. Its ease of integration with existing systems permits SecureCore technology to serve as a platform for future civilian and military mobile computing/communication devices.