The CyberSMART™ suite of cyber exercise tools is a Web-based system that includes a Scenario Planning Module, an Exercise Execution Engine, and a new Test Range Controller concept. The Test Range Controller will extend CyberSMART’s capabilities to support live, full-scale exercises at cyber test ranges.

SCENARIO PLANNING
The CyberSMART Scenario Planning Module (SPM) is a scalable cyber exercise planning tool built on the Homeland Security Exercise and Evaluation Program (HSEEP) methodology. The SPM provides a structured, computer-assisted environment for identifying exercise objectives and building the scenario gamespace. It allows a widely dispersed team of scenario developers to efficiently collaborate and capture the information necessary to plan complex cyber incident preparedness exercises. Exercise planners can easily create themes and problem chains, and can characterize the participating organizations’ technology assets and underlying transactions, leading to effective Master Scenario Events Lists (MSELs).

Unlike generic emergency response exercise tools, CyberSMART is designed specifically to address challenges unique to the execution of exercises containing major cyber elements. It enables planners to construct enough technical content around a MSEL to make an effective, realistic cyber exercise. Teams can develop and validate cyber scenario elements to ensure that they are logical, do not conflict, and meet the specific exercise objectives.

EXERCISE CONDUCT
When conducting cyber exercises, the CyberSMART Exercise Engine (EEE) is used to provide participants with exercise injects from the MSEL generated during the planning phase. It enables an Exercise Controller to manage the MSEL and the exercise by controlling scenario time and dynamically changing the MSEL injects as necessary. The CyberSMART EEE creates an immersive environment in which participants can build situational awareness based on indicators and warnings extracted from the scenario events, while maintaining the IT asset landscape that was developed in the planning phase. Participants provide responses to threats as they are identified. Responses are based on organizational strategies and can be analyzed in after-action review.

TEST RANGE CONTROL
The Space Dynamics Laboratory (SDL) is developing a prototype Test Range Controller (TRC) that will serve as an interface between the CyberSMART planning and execution tools and cyber test ranges. The TRC will allow users to design realistic and useful cyber exercises in CyberSMART and then carry out the behaviors defined in the exercise on a functional test range. It does this by exposing the range IT assets (hardware), target vectors, and behaviors to CyberSMART via a range driver. CyberSMART can then notify the test range driver of the behaviors to express on the range. At timed or user-triggered events, CyberSMART will inject behavior into the system via the TRC. With respect to participant responses, the test range driver may provide feedback into the system. Custom drivers can be developed to support specific test ranges, including networks of virtual machines, physical hardware, Supervisory Control And Data Acquisition (SCADA) Industrial Control Systems (ICS), or spacecraft simulators.