Objective

An objective, reliable, repeatable basis for evaluating cybersecurity resilience is needed. A cybersecurity resilience framework facilitates discussion and decision making among stakeholders and cybersecurity practitioners, allows comparisons between system configurations, and enables the creation of minimum acceptable performance thresholds.

Approach

We propose the term “resilience posture” to describe the relatively persistent state of an entire cyber system. Resilience posture is a high-level quantifiable system attribute that remains consistent within policy and management decision cycles. The degree to which the system is configured to be resilient considers its intended purpose, its known hazard environment, its assessment of the future, and its values. These attributes are incorporated into a resilience framework to enable the assessment of a system’s resilience posture.

The evaluation of cyber system resilience requires two types of measurements. First, the system must monitor various operational conditions. These measurements are critical to identify and respond to disruptions and to enable a robust system. These measurements are part of one or more observation, orientation, decision, and action (OODA) loops that fall along a spectrum of autonomy from fully automated to human-supervised. The second type consists of measurements about how well the OODA processes cover the critical system functions and the hazards to which the system is exposed. They allow assessment of how well system management processes anticipate, mitigate, and adapt to a changing environment. The assessment, decision, and change processes loop exists outside of this OODA control loop.

Family of Resilience Metrics
**Achievements**

- Developed a theoretical framework, in the form of definitions, a model, and a syntax, to provide a mechanism for bridging resilience management process models (e.g., CERT-RMM) and the many enumerations of cyber-defense metrics that have been proposed (MITRE, CIS)
- Developed an initial list of measures of resilience from literature and subject matter expert elicitation
- Developed a resilience taxonomy as a knowledge representation tool and to provide a basis for discussion
- Initiated scoping studies to develop test procedures and focus future efforts
- Developed a test plan and procedures to implement measures in the cybersecurity testbed

**Impact**

The proposed resilience framework enables strategic and tactical approaches to system resilience and facilitates discussion among stakeholders and cybersecurity practitioners regarding the necessary features and measures of system resilience. The framework also fills an identified gap in the literature between high-level process management and low-level control systems literature. The development of a resilience taxonomy continues to foster discussion and harmonization of terminology.

**Future Work**

In FY 2015, we will continue implementation of measures in the testbed, evaluate the quality and utility of the measures, and combine measures to develop metrics for cybersecurity resilience. A three-pronged approach will be utilized for measures evaluation: descriptive case study, low-resolution descriptive modeling and simulation, and high resolution implementation in the testbed. The resilience framework will be submitted to peer-reviewed literature.