Cybersecurity Framework Performance Goals August 28, 2013

Background:

Executive Order 13636 directs Federal agencies to coordinate the development and implementation of a prioritized, repeatable, flexible and cost effective cybersecurity framework (Framework) presently under development by the National Institute of Standards and Technology (NIST). Section 7(d) of Executive Order 13636 requires the Secretary of Homeland Security to provide performance goals (Performance Goals) for the Cybersecurity Framework (Framework) developed by NIST.

The Performance Goals are applicable to organizations adopting the Framework, including but not limited to infrastructure designated as Cyber-Dependent under Section 9 of EO 13636. They are intended to encourage progress toward national-level outcomes achieved in part by widespread adoption of the Framework, and stress the importance of an enterprise risk management strategy that associates cybersecurity investments with enterprise business plans.

Organizations should view the Performance Goals as guideposts to adopting the Framework that will encourage movement in a common direction and promote the reliability and integrity of critical functions[1] in the face of most cyber incidents.

Performance Goals

The Cybersecurity Framework is adopted such that:

- PG 1: Critical systems and functions are identified and prioritized and cyber risk is understood as part of a risk management plan.
- PG 2: Risk-informed actions are taken to protect critical systems and functions.
- PG 3: Adverse cyber activities are detected and situational awareness of threats is maintained.
- PG 4: Resources are coordinated and applied to triage and respond to cyber events and incidents in order to minimize impacts to critical systems and functions.
- PG 5: Following a cyber incident, impacted critical systems and functions are reconstituted based on prior planning and informed by situational awareness.
- PG 6: Security and resilience are continually improved based on lessons learned consistent with risk management planning.

[1] Critical functions are sets of processes that produce, provide, and maintain a sector’s products and services; they should not be confused with the Framework Functions (Identify, Protect, Detect, Respond, Recover)

Key Terms:

Critical functions: Sets of processes that produce, provide, and maintain a sector's products and services.

Critical Infrastructure: Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.