Policy

Proficiency Code: B

There are many documents pertaining to cyberspace operations policy. The documents most relevant to Air Force cyberspace operations are in AFDD 3–12 *Cyberspace Operations, Appendix B, Policy and Doctrine Related to Cyberspace Operations.*

National policy - The *National Strategy to Secure Cyberspace* is the comprehensive strategy for the US to secure cyberspace. It spells out three strategic priorities:

- Prevent cyber-attacks against America's critical infrastructure
- Reduce national vulnerability to cyber attacks
- Minimize damage and recover time from cyber attacks

The ***National Strategy to Secure Cyberspace*** outlines the framework for organizing and prioritizing US Government efforts in cyberspace. This strategy guides federal government departments and agencies that secure cyberspace. It identifies the steps every individual can take to improve our collective cyberspace security. More information on the national policy can be found at the Department of Homeland Security's website http://www.dhs.gov.

The ***National Military Strategy for Cyberspace Operations*** (NMS-CO) is the comprehensive strategy for US Armed Forces to ensure US superiority in cyberspace. There are four strategic priorities of the NMS-CO:

- Gain and maintain initiative to operate within adversary decision cycles.
- Integrate cyberspace capabilities across the range of military operations (ROMO).
- Build capacity for cyberspace operations.
- Manage risk for operations in cyberspace.

The NMS-CO describes the cyberspace domain, articulates cyberspace threats and vulnerabilities, and provides a strategic framework for action. The NMS-CO is the US Armed Forces' comprehensive strategic approach for using cyberspace operations to assure US military strategic superiority in the domain. The integration of offensive and defensive cyberspace operations, coupled with the skill and knowledge of our people, is fundamental to this approach.