Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 1 reference coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

response and recovery

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 1 reference coded [ 0.30% Coverage]

Reference 1 - 0.30% Coverage

Joint Forces will secure the ‘.mil’ domain, requiring a resilient DoD cyberspace architecture that employs a combination of detection, deterrence, denial, and multi-layered defense. We will improve our cyberspace capabilities so they can often achieve significant and proportionate effects with less cost and lower collateral impact.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 2 references coded [ 0.02% Coverage]

Reference 1 - 0.02% Coverage

the Department’s prevent-and-deter activities will be focused on ensuring a defense in depth of the United States;

Reference 2 - 0.01% Coverage

DoD must actively defend its networks.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 2 references coded [ 0.23% Coverage]

Reference 1 - 0.04% Coverage

could rapidly react to a cyber attack on the nation.

Reference 2 - 0.19% Coverage

These capabilities, matched with the expertise of the Intelligence Community and the Department of Defense, reflect a “whole-of-government” approach to identify, mitigate, and defend against cyber incidents and national-level events