Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 3 references coded [ 0.12% Coverage]

Reference 1 - 0.02% Coverage

prevent, and respond to significant cybersecurity incidents

Reference 2 - 0.07% Coverage

The strategy also must include prevention, mitigation, and response against threats to or subversion of the people who operate and benefit from the infrastructure, the processes that run or take advantage of the infrastructure, and the supply chains used to build and maintain the infrastructure

Reference 3 - 0.03% Coverage

Develop a process between the government and the private sector to assist in preventing, detecting, and responding to cyber incidents.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2010\_national\_security\_strategy - § 3 references coded [ 0.08% Coverage]

Reference 1 - 0.03% Coverage

drew a swift and forceful response from the United States and our allies and partners in Afghanistan

Reference 2 - 0.01% Coverage

response to cyber attacks

Reference 3 - 0.04% Coverage

Our strategy to attack these networks must respond in kind and target their illicit resources and access to the global financial system through financial measures,

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 2 references coded [ 0.19% Coverage]

Reference 1 - 0.17% Coverage

We will, on order, be prepared to respond to any attack across the full spectrum of military capabilities with an appropriate and measured response at a time and place of our Nation’s choosing.

Reference 2 - 0.02% Coverage

threat of retaliation

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\QDR as of 29JAN10 1600 - § 1 reference coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

supporting a response to an attack