Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 2 references coded [ 0.63% Coverage]

Reference 1 - 0.46% Coverage

Co-location and dual-hatting of these separate and distinct   
Given its need to ensure the ability to operate Department of Defense Strategy for Operating in Cyberspace 5   
organizations allow DoD, and the U.S. government, to maximize talent and capabilities, leverage respective authorities, and operate more effectively to achieve DoD’s mission.

Reference 2 - 0.17% Coverage

This   
cultural shift will be enabled by new policies, new methods of personnel training, and innovative workforce communications.

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

Reference 1 - 0.10% Coverage

We must seek executive and Congressional action to provide new authorities to enable effective action in cyberspace.

Reference 2 - 0.08% Coverage

We seek authorities for a pooled-resources approach to facilitate more complementary efforts

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 6 references coded [ 1.84% Coverage]

Reference 1 - 0.23% Coverage

In February 2013, President Obama signed Executive Order (E.O.) 13636 on Improving Critical Infrastructure Cybersecurity that, among other actions, directed the National Institute of Standards and Technology (NIST) to lead a process to develop a template of cybersecurity best practices.

Reference 2 - 0.45% Coverage

The Cross-Agency Priority goal framework was established by the GPRA Modernization Act of 2010 and is used to accelerate progress on a limited number of Presidential priority areas where implementation will require collaboration and coordinated action by multiple departments and agencies. Each goal has a named senior leader both within the Executive Office of the President and within key departments and agencies. Additional information on the Cross-Agency Priority goals for cybersecurity can be found here: http://www.performance.gov/cap-goals-list/.

Reference 3 - 0.49% Coverage

In 2013, the Administration issued Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, which focused on advancing a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. E.O. 13636, which was issued at the same time as PPD-21, furthered efforts to protect critical infrastructure. E.O. 13636 requirement information sharing on cyber threats among Federal agencies and with the private sector and through the development of the Cybersecurity Framework, which a number of Federal agencies are seeking to adopt.

Reference 4 - 0.25% Coverage

Further, in April 2015 the President issued a new Executive Order authorizing the imposition of sanctions on individuals and entities whose cyberenabled activities have contributed to a significant threat to the national security, foreign policy, or economic health or financial stability of the United States.

Reference 5 - 0.18% Coverage

In establishing this new policy, the Administration is creating a means of imposing economic costs against not just those that conduct cyber attacks, but those responsible for supporting, enabling, or ordering such attacks.

Reference 6 - 0.22% Coverage

Presidential Policy Directive 20 provides a policy framework to govern the conduct of such cyber operations. Even though the United States Government is not limited to responding to a cyber attack through cyberspace, there are unique advantages to such a symmetrical response.