Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 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\\CS1\_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\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 11 references coded [ 1.90% Coverage]

Reference 1 - 0.18% Coverage

DoD will focus on ensuring that its forces are trained and ready to operate using the capabilities and architectures they need to conduct cyber operations, continue to build policy and legal frameworks to govern CMF employment, and integrate the CMF into DoD’s overall planning and force development.

Reference 2 - 0.16% Coverage

Because of the variety and number of state and non-state cyber actors in cyberspace and the relative availability of destructive cyber tools, an effective deterrence strategy requires a range of policies and capabilities to affect a state or non-state actors’ behavior.

Reference 3 - 0.10% Coverage

The Defense Department will integrate cybersecurity requirements and assessments into the DoD Mission Assurance program and update DoD policy appropriately.

Reference 4 - 0.08% Coverage

Acquisition and procurement policy and practice will be updated to promote effective cybersecurity throughout a system’s life cycle.

Reference 5 - 0.19% Coverage

Improve accountability and responsibility for the protection of data across DoD and the DIB. The Defense Department will ensure that policies and any associated federal rules or contract language requirements have been implemented to require DIB companies to report data theft and loss to the Defense Cyber Crime Center.

Reference 6 - 0.26% Coverage

Use DoD counterintelligence capabilities to defend against intrusions. The Military Departments and the Under Secretary of Defense for Intelligence, in consultation with the Principal Cyber Advisor, will develop a strategy for the Secretary of Defense’s approval that maximizes the capabilities and authorities of the military departments’ counterintelligence agencies to identify, attribute, and defend against cyber intruders.

Reference 7 - 0.08% Coverage

Counterintelligence authorities are uniquely positioned to improve our insight into and frustrate and defeat cyber espionage.

Reference 8 - 0.10% Coverage

DoD will work with other U.S. government agencies and Congress to support legislation that enables information sharing between the U.S. government and the private sector.

Reference 9 - 0.30% Coverage

Establish the Office of the Principal Cyber Advisor to the Secretary of Defense. In the National Defense Authorization Act (NDAA) of 2014, Congress required the Defense Department to designate a Principal Cyber Advisor to the Secretary of Defense to review military cyberspace activities, cyber mission forces, and offensive and defensive cyber operations and missions. In addition, the Principal Cyber Advisor will govern the development of DoD cyberspace policy and strategy for the DoD enterprise.

Reference 10 - 0.15% Coverage

The diffuse nature of the DoD cyber budget presents DoD with a challenge for effective budgetary management; DoD must develop a new method for managing cross-program funding to improve mission effectiveness and achieve management efficiencies.

Reference 11 - 0.31% Coverage

Develop DoD’s cyber operations and   
Sailors conduct an exercise at Fleet Cyber Command’s headquarters in the Frank B. Rowlett Building, Fort George G. Meade, MD. This exercise features members of Fleet Cyber Command’s Joint Force Headquarters-Cyber (JFHQ-C).   
cybersecurity policy framework. Consistent with Presidential guidance, DoD will align and simplify its cyber operations and cybersecurity policy management and identified gaps, overlaps, seams, conflicts, and areas in need of revision in current documentation.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 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.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 7 references coded [ 1.66% Coverage]

Reference 1 - 0.21% Coverage

The Administration will clarify the relevant authorities, responsi-   
bilities, and accountability within and across departments and agencies for securing Federal information systems, while setting the standard for effective cybersecurity risk management

Reference 2 - 0.38% Coverage

We will continue to deploy centralized capabilities, tools, and services through DHS where appropriate, and improve oversight and compliance with applicable laws, policies,   
standards, and   
directives. This will likely require new policies and architectures that enable the government to better leverage innovation. DOD and the IC will consider these activities as they work to better secure national security systems, DOD systems, and IC systems, as appropriate.

Reference 3 - 0.16% Coverage

It also includes   
addressing deficiencies in the Federal acquisition system, such as providing more streamlined authorities to exclude risky vendors, products, and services when justified.

Reference 4 - 0.27% Coverage

The Administration will push to ensure that our Federal departments and agencies have the necessary legal authorities and resources to combat transnational cybercriminal activity, including identifying and dismantling botnets, dark markets, and other infrastructure used to enable cybercrime, and combatting economic espionage

Reference 5 - 0.27% Coverage

The Administration will work with the Congress to update electronic surveillance and computer crime statutes to enhance law enforcement’s capabilities to lawfully gather necessary evidence of criminal activity, disrupt criminal infrastructure through civil injunctions, and impose appropriate consequences upon malicious

Reference 6 - 0.21% Coverage

The Administration will leverage the President’s proposed merit-based immigration reforms to ensure that the United States has the most competitive technology sector. This effort may require additional legislation to achieve the sought after goals.

Reference 7 - 0.17% Coverage

This Administration will issue transformative policies that reflect today’s new reality and guide the United States Government   
towards strategic outcomes that   
protect the American people and our way of life.