Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review - § 1 reference coded [ 0.05% Coverage]

Reference 1 - 0.05% Coverage

First, it builds on the Defense Strategic Guidance, published in 2012, by outlining an updated defense strategy that protects and advances U.S. interests and sustains U.S. leadership

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 19 references coded [ 3.36% Coverage]

Reference 1 - 0.43% Coverage

DoD sets five strategic goals for its cyberspace missions: 1. Build and maintain ready forces and capabilities to conduct cyberspace operations;   
2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;   
7   
Th e De pa r tme n t o f De f e n s e Cy be r S t r a t e g y   
3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;   
4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;   
5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

Reference 2 - 0.12% Coverage

To mitigate risks and defend U.S. interests in the current and future security environment, the Defense Department outlines five strategic goals and specific objectives for its activities and missions.

Reference 3 - 0.06% Coverage

STRATEGIC GOAL I: BUILD AND MAINTAIN READY FORCES AND CAPABILITIES TO CONDUCT CYBERSPACE OPERATIONS.

Reference 4 - 0.06% Coverage

STRATEGIC GOAL II: DEFEND THE DOD INFORMATION NETWORK, SECURE DOD DATA, AND MITIGATE RISKS TO DOD MISSIONS.

Reference 5 - 0.09% Coverage

STRATEGIC GOAL III: BE PREPARED TO DEFEND THE U.S. HOMELAND AND U.S. VITAL INTERESTS FROM DISRUPTIVE OR DESTRUCTIVE CYBERATTACKS OF SIGNIFICANT CONSEQUENCE.

Reference 6 - 0.10% Coverage

STRATEGIC GOAL IV: BUILD AND MAINTAIN VIABLE CYBER OPTIONS AND PLAN TO USE THOSE OPTIONS TO CONTROL CONFLICT ESCALATION AND TO SHAPE THE CONFLICT ENVIRONMENT AT ALL STAGES.

Reference 7 - 0.10% Coverage

STRATEGIC GOAL V: BUILD AND MAINTAIN ROBUST INTERNATIONAL ALLIANCES AND PARTNERSHIPS TO DETER SHARED THREATS AND INCREASE INTERNATIONAL SECURITY AND STABILITY.

Reference 8 - 0.06% Coverage

Each of DoD’s strategic goals requires specific, measurable objectives for the Department to achieve.

Reference 9 - 0.35% Coverage

The Office of the Principal Cyber Advisor to the Secretary of Defense, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Joint Staff will work with DoD components to prioritize and oversee the implementation of this strategy and its objectives and to assign offices of primary and support responsibility for managing each objective. The office of primary responsibility will develop a project plan for each objective; the Principal Cyber Advisor will track progress in achieving each objective and ultimately the success of each strategic goal.

Reference 10 - 0.06% Coverage

STRATEGIC GOAL I: BUILD AND MAINTAIN READY FORCES AND CAPABILITIES TO CONDUCT CYBERSPACE OPERATIONS.

Reference 11 - 0.06% Coverage

STRATEGIC GOAL II: DEFEND THE DOD INFORMATION NETWORK, SECURE DOD DATA, AND MITIGATE RISKS TO DOD MISSIONS.

Reference 12 - 0.09% Coverage

STRATEGIC GOAL III: BE PREPARED TO DEFEND THE U.S. HOMELAND AND U.S. VITAL INTERESTS FROM DISRUPTIVE OR DESTRUCTIVE CYBERATTACKS OF SIGNIFICANT CONSEQUENCE.

Reference 13 - 0.10% Coverage

STRATEGIC GOAL IV: BUILD AND MAINTAIN VIABLE CYBER OPTIONS AND PLAN TO USE THOSE OPTIONS TO CONTROL CONFLICT ESCALATION AND TO SHAPE THE CONFLICT ENVIRONMENT AT ALL STAGES.

Reference 14 - 0.10% Coverage

STRATEGIC GOAL V: BUILD AND MAINTAIN ROBUST INTERNATIONAL ALLIANCES AND PARTNERSHIPS TO DETER SHARED THREATS AND INCREASE INTERNATIONAL SECURITY AND STABILITY.

Reference 15 - 0.31% Coverage

To achieve the goals and objectives outlined in this strategy will require hard choices regarding cyber forces and personnel, organizations, and capabilities. The financial choices that DoD makes in the course of implementing this strategy will have national and global implications for years to come, and DoD must operate in an effective and cost-efficient manner to guarantee the best return on its investments. To that end, DoD will pursue the following management objectives to govern its cyber activities and missions.

Reference 16 - 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 17 - 0.09% Coverage

Improve cyber budgetary management. DoD will develop an agreed-upon method to more transparently and effectively manage the DoD cyber operations budget.

Reference 18 - 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.

Reference 19 - 0.55% Coverage

Conduct an end-to-end assessment of DoD’s cyber capabilities. U.S. Cyber Command will lead a comprehensive operational assessment of its posture. In coordination with the Principal Cyber Advisor to the Secretary of Defense, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Office of the Director of Coast Assessment and Program Evaluation, USCYBERCOM will provide short- and long-term recommendations through the CIMB to provide to the Secretary of   
30   
Th e De pa r tme n t o f De f e n s e Cy be r S t r a t e g y   
Defense regarding organizational structure, command and control mechanism, rules of engagement, personnel, capabilities, tools, and potential operational gaps. The goal of this posture assessment will be to provide a clear understanding of the future operational environment; key stakeholder views; as well as strategic priorities, choices, and resources for planning and operations.