Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2010\_national\_security\_strategy - § 2 references coded [ 0.10% Coverage]

Reference 1 - 0.04% Coverage

That is why we must also enhance our resilience—the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

Reference 2 - 0.06% Coverage

we are working across the government and with the private sector to design more secure technology that gives us the ability to better protect and to improve the resilience of critical government and industry systems and networks

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011 DOD Strategy for Operating in Cy - § 2 references coded [ 0.83% Coverage]

Reference 1 - 0.60% Coverage

These efforts will be supported by the development of increasingly resilient networks and systems. In the case of a contingency involving network failure or significant compromise, DoD must be able to remain operationally effective by isolating and neutralizing the impact, using redundant capacity, or shifting its operations from one system to another. Multiple networks can add diversity, resiliency, and mission assurance to cyberspace operations.

Reference 2 - 0.23% Coverage

To foster resiliency and smart diversity in its networks and systems, DoD will explore new and innovative approaches and paradigms for both existing and emerging challenges.

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011-national-military-strategy - § 3 references coded [ 0.31% Coverage]

Reference 1 - 0.08% Coverage

maintain joint assured access to the global commons and cyberspace should they become contested

Reference 2 - 0.14% Coverage

Joint assured access to the global commons and cyberspace constitutes a core aspect of U.S. national security and remains an enduring mission for the Joint Force.

Reference 3 - 0.08% Coverage

Joint Forces will secure the ‘.mil’ domain, requiring a resilient DoD cyberspace architecture

Files\\2011 Case Study\\Primary Sources\_Policy\_Strategies\\2011\_International\_strategy\_for\_cyberspace - § 4 references coded [ 0.13% Coverage]

Reference 1 - 0.03% Coverage

resilient to arbitrary or malicious disruption

Reference 2 - 0.03% Coverage

national and international network resilience

Reference 3 - 0.05% Coverage

Ensuring the resilience of our networks and information systems

Reference 4 - 0.02% Coverage

enhance overall resilience

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2014 Quadrennial Defense Review CLEAN - § 2 references coded [ 0.02% Coverage]

Reference 1 - 0.01% Coverage

more resilient systems and system architectures

Reference 2 - 0.01% Coverage

resilient architectures,

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Military Strategy CLEAN - § 2 references coded [ 0.10% Coverage]

Reference 1 - 0.05% Coverage

reliable and resilient communications links

Reference 2 - 0.04% Coverage

sustaining a resilient global posture

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 National Security Strategy CLEAN - § 7 references coded [ 0.49% Coverage]

Reference 1 - 0.04% Coverage

These actions are a part of our resilience at home and a source of our influence abroad.

Reference 2 - 0.12% Coverage

Going forward, we will strengthen our foundation by growing our economy, modernizing our defense, upholding our values, enhancing the resilience of our homeland, and promoting talent and diversity in our national security workforce.

Reference 3 - 0.03% Coverage

make sure America is resilient in the face of adversity

Reference 4 - 0.13% Coverage

We are working with the owners and operators of our Nation’s critical cyber and physical infrastructure across every sector—financial, energy, transportation, health, information technology, and more—to decrease vulnerabilities and increase resilience

Reference 5 - 0.05% Coverage

Prosperity and security increasingly depend on an open, interoperable, secure, and reliable Internet.

Reference 6 - 0.09% Coverage

we are securing Federal networks and working with the private sector, civil society, and other stakeholders to strengthen the security and resilience of U.S. critical infrastructure

Reference 7 - 0.03% Coverage

enhance the resiliency of critical U.S. space capabilities.

Files\\2015 Case Study\\Primary Sources\_Policy\_Strategies\\2015 WH Report on Cyber Deterrence Policy Final CLEAN - § 14 references coded [ 2.26% Coverage]

Reference 1 - 0.01% Coverage

Resiliency,

Reference 2 - 0.13% Coverage

To make these deterrence efforts credible, we must deploy strong defenses and architect resilient systems that recover quickly from attacks or other disruptions.

Reference 3 - 0.20% Coverage

Pursuing defense, resiliency, and reconstitution initiatives to provide critical networks with a greater capability to prevent or minimize the impact of cyber attacks or other malicious cyber activity, and reconstitute rapidly if attacks succeed.

Reference 4 - 0.19% Coverage

Building strong partnerships with the private sector to promote cybersecurity best practices; assist in building public confidence in cybersecurity measures; and lend credibility to national efforts to increase network resiliency.

Reference 5 - 0.23% Coverage

In particular, there should be certainty about the fact that, even in the face of sophisticated cyber threats, the United States can maintain robust defenses, ensure resilient networks and systems, and implement a robust response capability that can project power and secure U.S. interests.

Reference 6 - 0.03% Coverage

Defense, Resiliency, and Reconstitution

Reference 7 - 0.24% Coverage

Further, the United States Government invests heavily in improving its own information security and ensuring the resiliency of vital computer systems and networks, including developing the ability to reconstitute them rapidly, operate them in degraded states, or function without them if necessary.

Reference 8 - 0.11% Coverage

In addition to defensive measures, the United States Government must also ensure the resiliency of its networks, systems and data.

Reference 9 - 0.22% 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.

Reference 10 - 0.24% Coverage

Such efforts to improve cybersecurity information sharing and risk management within the government can strengthen both situational awareness and indications and warning, which in turn can help government network defenders prepare for attacks and improve the resilience of government systems.

Reference 11 - 0.25% Coverage

The United States Government is also working with its counterparts around the world to enhance deterrence by expanding bilateral and multilateral defense and security relationships to include greater cooperation in the areas of network defense, information sharing, incident response, and resiliency.

Reference 12 - 0.11% Coverage

To keep pace, the United States Government must evolve and develop innovative solutions to make cyberspace resilient to future threats

Reference 13 - 0.08% Coverage

continue to improve the resilience of U.S. computers, networks, and critical infrastructure

Reference 14 - 0.22% Coverage

A credible U.S. cyber deterrent will require sustained efforts by all elements of the government to pursuing policies and capabilities that improve network defenses, bolster the Nation’s cyber resiliency, and provide options for imposing costs on malicious cyber actors.