Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 1 reference coded [ 0.15% Coverage]

Reference 1 - 0.15% Coverage

We continue to emphasize that systematically adopting sound information technology practices—across the public and private sectors—will reduce our Nation’s vulnerabilities and strengthen networks and systems~

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 1 reference coded [ 0.07% Coverage]

Reference 1 - 0.07% Coverage

And too many governments are responding to the expansion of civil society and free press by passing laws and adopting policies that erode that progress.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 2 references coded [ 0.75% Coverage]

Reference 1 - 0.57% Coverage

U.S. companies have begun to adopt and implement the Framework across many different sectors of the economy.6 This adoption means that many organizations are raising their overall cybersecurity baseline by implementing standards-based measures to protect their most sensitive information, close known vulnerabilities in their networks, and invest in the hardware and software necessary for basic cyber defense. The Administration will continue to promote the adoption of the Framework as a key means of improving U.S. cyber defenses and, by extension, decreasing adversaries’ perceptions of the benefits to be gained from engaging in malicious cyber activities against U.S. computers and networks.

Reference 2 - 0.18% Coverage

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.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 1 reference coded [ 0.09% Coverage]

Reference 1 - 0.09% Coverage

ADOPT NEW TRADE AND INVESTMENT AGREEMENTS AND MODERNIZE EXISTING ONES: The United States will pursue bilateral trade and investment agreements with countries that commit to fair and reciprocal trade and will modernize existing agreements to ensure they are consistent with those principles.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 7 references coded [ 1.48% Coverage]

Reference 1 - 0.28% Coverage

Further, as recommended in the   
E.O. 13800 Report to the President on Federal IT Modernization,   
the Administration will support   
N AT I O N A L C Y BE R S T R AT E G Y   
adoption of consolidated acquisition strategies to improve cybersecurity and reduce overhead costs associated with using inconsistent contract provisions across the Federal Government.

Reference 2 - 0.18% Coverage

The United States must be at the forefront of protecting communications by supporting rapid adoption of these forthcoming NIST standards across government infrastructure and by encouraging the Nation to do the same.

Reference 3 - 0.17% Coverage

Finally, we will work to expand the international consensus favoring the Convention on Cybercrime of the Council of Europe (Budapest Convention), including by supporting greater adoption of the convention.

Reference 4 - 0.18% Coverage

The Administration will work across stakeholder groups, including the private sector and civil society, to promote best practices and develop strategies to overcome market barriers to the adoption of secure technologies.

Reference 5 - 0.30% Coverage

Finally, the Administration will collaborate with international partners to promote open, industry-driven standards with government support, as appropriate, and risk-based approaches to address cybersecurity challenges to include platform and managed service approaches that lower barriers to secure practice adoption across the breadth of the ecosystem.

Reference 6 - 0.20% Coverage

We will collaborate with the private sector and civil society to understand trends in technology advancement to maintain the United States technological edge in connected technologies and to ensure secure practices are adopted from the outset.

Reference 7 - 0.18% Coverage

Finally, the United States will work with international partners, government, industry, civil society, technologists, and academics to improve the adoption and awareness of cybersecurity best practices worldwide.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 1 reference coded [ 0.05% Coverage]

Reference 1 - 0.05% Coverage

NATO also adopted a broad new agenda at the 2022 Madrid Summit to address systemic challenges from the PRC and other security risks from cyber to climate

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 5 references coded [ 0.68% Coverage]

Reference 1 - 0.15% Coverage

In setting cybersecurity regulations for critical infrastructure, regulators are encouraged to drive the adoption of secure-by-   
NAT I ONAL CY B E RS E CU RI T Y S T RATEGY 8   
        
design principles, prioritize the availability of essential services, and ensure that systems are designed to fail safely and recover quickly.

Reference 2 - 0.19% Coverage

The Administration will prioritize adoption and enforcement of a risk-based approach to cybersecurity across Infrastructure-as-a-Service providers that addresses known methods and indicators of malicious activity including through implementation of EO 13984, “Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities.”

Reference 3 - 0.10% Coverage

Continued disruptions of critical infrastructure and thefts of personal data make clear that market forces alone have not been enough to drive broad adoption of best practices in cybersecurity and resilience.

Reference 4 - 0.09% Coverage

To further incentivize the adoption of secure software development practices, the Administration will encourage coordinated vulnerability disclosure across all technology types and sectors

Reference 5 - 0.15% Coverage

The Federal Government will lead by ensuring that its networks have implemented these and other security measures while partnering with stakeholders to develop and drive adoption of solutions that will improve the security of the Internet ecosystem and support research to understand and address reasons for slow adoption.