Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 8 references coded [ 0.19% Coverage]

Reference 1 - 0.03% Coverage

standards that establishes certain rights and responsibilities for all sovereign nations

Reference 2 - 0.05% Coverage

The United States must reserve the right to act unilaterally if necessary to defend our nation and our interests, yet we will also seek to adhere to standards that govern the use of force

Reference 3 - 0.03% Coverage

Doing so strengthens those who act in line with international standards, while isolating and weakening those who do not.

Reference 4 - 0.03% Coverage

engagement with the transpacific partnership countries to shape a regional agreement with high standards.

Reference 5 - 0.01% Coverage

international standards

Reference 6 - 0.01% Coverage

we must have clear, defensible, and lawful standards

Reference 7 - 0.02% Coverage

hold ourselves to the same standards that we apply to other nations

Reference 8 - 0.01% Coverage

strengthening of international norms and standards.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 17 references coded [ 0.91% Coverage]

Reference 1 - 0.02% Coverage

International Standards

Reference 2 - 0.12% Coverage

The United States is committed to international initiatives and standards that enhance cybersecurity while safeguarding free trade and the broader free flow of information

Reference 3 - 0.06% Coverage

develop new standards for information systems that make networks faster and more reliable,

Reference 4 - 0.05% Coverage

international standards for information and communication technology

Reference 5 - 0.06% Coverage

Vulnerability reduction will require robust technical standards and solutions

Reference 6 - 0.05% Coverage

supporting the soundest technical standards and governance structures,

Reference 7 - 0.03% Coverage

Promoting International Standards

Reference 8 - 0.01% Coverage

standards

Reference 9 - 0.05% Coverage

Respecting the international standards of technology development and trade

Reference 10 - 0.02% Coverage

secure technical standards,

Reference 11 - 0.02% Coverage

cybersecurity standards

Reference 12 - 0.11% Coverage

deploying products, processes, and services based upon such standards are the basis of an interoperable, secure and resilient global infrastructure~

Reference 13 - 0.18% Coverage

The public and private sectors must work together to develop, maintain, and implement these standards and support the development of international standards and conformity assessment schemes that prevent barriers to international trade and commerce~

Reference 14 - 0.03% Coverage

International cybersecurity standardization

Reference 15 - 0.03% Coverage

international standards-based requirements

Reference 16 - 0.04% Coverage

shared understanding of standard operating procedures

Reference 17 - 0.03% Coverage

best practices and technical standards

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 1 reference coded [ 0.13% Coverage]

Reference 1 - 0.13% Coverage

Seeking to adhere to international standards, the United States will use military force in concert with allies and partners whenever possible

Files\\2011 Case Study\\CS1\_Secondary Sources\_Authoritative\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 12 references coded [ 0.08% Coverage]

Reference 1 - 0.01% Coverage

standards

Reference 2 - 0.01% Coverage

uter netw

Reference 3 - 0.02% Coverage

standards regarding the security of and operations in cyberspace

Reference 4 - 0.01% Coverage

standards.

Reference 5 - 0.02% Coverage

mprove the security of interoperable networks through the development of global standards,

Reference 6 - 0.01% Coverage

international standards bodies

Reference 7 - 0.01% Coverage

standards,

Reference 8 - 0.01% Coverage

standards

Reference 9 - 0.01% Coverage

standards.

Reference 10 - 0.01% Coverage

standards

Reference 11 - 0.01% Coverage

standards,

Reference 12 - 0.01% Coverage

standards of conduct in cyberspace.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 2 references coded [ 0.45% Coverage]

Reference 1 - 0.20% Coverage

DoD will continue to assess Defense Federal Acquisition Regulation Supplement (DFARS) rules and associated guidance to ensure they mature over time in a manner consistent with known standards for protecting data from cyber adversaries, to include standards promulgated by the National Institute of Standards and Technology (NIST).

Reference 2 - 0.26% Coverage

Strengthen DoD’s procurement and acquisition cybersecurity standards. To defend DoD networks, DoD must strengthen the cybersecurity requirements of DoD’s network acquisition and procurement items by integrating cybersecurity standards into contract vehicles for research, development, and procurement. DoD will specify additional cybersecurity standards for industry to meet for components of any DoD procurement item.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Security Strategy - § 14 references coded [ 0.96% Coverage]

Reference 1 - 0.06% Coverage

We are shaping global standards for cybersecurity and building international capacity to disrupt and investigate cyber threats.

Reference 2 - 0.07% Coverage

It also means holding ourselves to international norms and standards that we expect other nations to uphold, and admitting when we do not

Reference 3 - 0.08% Coverage

Working with U.S. states and private utilities, we will set the first-ever standards to cut the amount of carbon pollution our power plants emit into the air.

Reference 4 - 0.11% Coverage

Building on the progress made in Copenhagen and in ensuing negotiations, we are working toward an ambitious new global climate change agreement to shape standards for prevention, preparedness, and response over the next decade.

Reference 5 - 0.05% Coverage

will continue to work with the Congress to pursue a legislative framework that ensures high standards.

Reference 6 - 0.09% Coverage

We have responsibilities at home to continue to improve our banking practices and forge ahead with regulatory reform, even as we press others to align with our robust standards.

Reference 7 - 0.04% Coverage

setting higher standards to level the playing field for American workers and firms.

Reference 8 - 0.05% Coverage

we are setting the world’s highest standards for labor rights and environmental protection

Reference 9 - 0.06% Coverage

it is essential we hold ourselves to the highest possible standard, even as we do what is necessary to secure our people.

Reference 10 - 0.05% Coverage

need for strong and consistent implementation of the international standards on combating illicit finance.

Reference 11 - 0.09% Coverage

The United States is leading the way in promoting adherence to standards of accountable and transparent governance, including through initiatives like the Open Government Partnership.

Reference 12 - 0.02% Coverage

raise global standards for trade.

Reference 13 - 0.09% Coverage

With Chile, Peru, Mexico, and Canada, we are setting new global trade standards as we grow a strong contingent of countries in the Americas that favor open trading systems to include TPP.

Reference 14 - 0.09% Coverage

We seek to advance our economic partnership with Brazil, as it works to preserve gains in reducing poverty and deliver the higher standards of public services expected by the middle class.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 7 references coded [ 1.37% Coverage]

Reference 1 - 0.11% Coverage

directed the National Institute of Standards and Technology (NIST) to lead a process to develop a template of cybersecurity best practices.

Reference 2 - 0.20% Coverage

In February 2014, NIST released the first version of the template, the Cybersecurity Framework (Framework), that references globally recognized standards and practices to help organizations understand, communicate, and manage their cyber risks.

Reference 3 - 0.11% Coverage

This adoption means that many organizations are raising their overall cybersecurity baseline by implementing standards-based measures

Reference 4 - 0.23% Coverage

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 5 - 0.28% Coverage

The Steering Committee, co-chaired by senior representatives of the Office of Management and Budget and the National Security Council staff, ensures senior-level accountability across departments and agencies for implementing policies and standards regarding the sharing and safeguarding of classified information on computer networks.

Reference 6 - 0.26% Coverage

The Executive Agent for Safeguarding, under the joint leadership of the Secretary of Defense and the Director of the National Security Agency, is developing effective technical safeguarding policies and standards addressing the safeguarding of national security systems and classified information within these systems.

Reference 7 - 0.17% Coverage

Such norms would also socialize standards of behavior in cyberspace consistent with each nation’s security interests and develop the international support necessary for collective action to counter bad actors

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 4 references coded [ 0.19% Coverage]

Reference 1 - 0.06% Coverage

We will set higher security standards to ensure that we keep dangerous people out of the United States and enhance our information collection and analysis to identify those who may already be within our borders.

Reference 2 - 0.03% Coverage

We will also work with international and industry partners to raise security standards.

Reference 3 - 0.04% Coverage

Agreements must adhere to high standards in intellectual property, digital trade, agriculture, labor, and the environment.

Reference 4 - 0.07% Coverage

Together we will emphasize fair trade enforcement actions when necessary, as well as multinational efforts to ensure transparency and adherence to international standards within trade and investment projects.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 National Cyber Strategy - § 17 references coded [ 3.02% Coverage]

Reference 1 - 0.06% Coverage

setting the standard for effective cybersecurity risk management.

Reference 2 - 0.18% Coverage

The Federal Government will ensure the systems it owns and operates meet the standards and cybersecurity best practices it recommends to industry.   
Projects   
that receive Federal funding must meet these standards as well.

Reference 3 - 0.11% Coverage

The Federal Government will also be a leader in developing and implementing standards and best practices in new and emerging areas.

Reference 4 - 0.26% Coverage

To protect against the potential threat of quantum computers being able to break modern public key cryptography, the Department of Commerce, through the National Institute of Standards and Technology (NIST), will continue to solicit, evaluate, and standardize quantum-resistant,   
public key cryptographic   
algorithms.

Reference 5 - 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 6 - 0.11% Coverage

We will promote an adaptable, sustainable, and secure technology supply chain that supports security based on best practices and standards.

Reference 7 - 0.15% Coverage

The Federal Government will continue to coordinate the development of cybersecurity standards and guidance to safeguard the electoral process and the tools that deliver a secure system.

Reference 8 - 0.22% Coverage

As the foundations of our   
economy are becoming increasingly rooted in digital technologies, the United States Government will model and promote standards that protect our economic security and reinforce the vitality of the American marketplace and American innovation.

Reference 9 - 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 10 - 0.21% Coverage

The United States Government will promote implementation and   
P I L L A R I I : PROM O T E A M E R I C A N PRO S P E R I T Y   
continuous updating of standards and best practices that deter and prevent current and evolving threats and hazards in all domains of the cyber ecosystem.

Reference 11 - 0.13% Coverage

These standards and practices should be outcome-oriented and based on sound technological principles rather than point-in-time company specifications

Reference 12 - 0.24% Coverage

The Administration will continue to work with international counterparts to promote open, industry driven standards, innovative products, and risk-based approaches that permit global innovation and the free flow of data while meeting the legitimate security needs of the United States.

Reference 13 - 0.30% Coverage

The United States Government will also leverage publicprivate collaboration to develop and circulate the NICE Framework, which provides a standardized approach for identifying cybersecurity workforce gaps, while also implementing actions to prepare, grow, and sustain a workforce that can defend and bolster America’s critical   
infrastructure and innovation base.

Reference 14 - 0.21% Coverage

International law and voluntary   
non-binding norms of responsible state behavior in cyberspace provide stabilizing, security-enhancing standards that define acceptable behavior to all states and promote greater predictability and stability in cyberspace.

Reference 15 - 0.07% Coverage

We will work to ensure that our approach to an open Internet is the international standard.

Reference 16 - 0.11% Coverage

The Administration will also support and promote open, industry-led standards activities based on sound technological principles.

Reference 17 - 0.20% Coverage

The United States will also advise on infrastructure deploy-   
N AT I O N A L C Y BE R S T R AT E G Y   
ments, innovation, risk management, policy, and standards to further the global Internet’s reach and to ensure interoperability, security, and stability.