Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2010 National Security Strategy - § 8 references coded [ 0.52% Coverage]

Reference 1 - 0.08% Coverage

Indeed, the basis for international   
★ 12 ★   
I I I . advaNCINg Our INTereSTS   
cooperation since World War II has been an architecture of international institutions, organizations, regimes, and 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 - 0.08% Coverage

We will pursue a trade agenda that includes an ambitious and balanced Doha multilateral trade agreement, bilateral and multilateral trade agreements that reflect our values and interests, and engagement with the transpacific partnership countries to shape a regional agreement with high standards.

Reference 5 - 0.10% Coverage

Our strategy to attack these networks must respond in kind and target their illicit resources and access to the global financial system through financial measures, administration and enforcement of regulatory authorities, outreach to the private sector and our foreign partners, and collaboration on international standards and information sharing.

Reference 6 - 0.04% Coverage

For detainees who cannot be prosecuted—but pose a danger to the American people—we must have clear, defensible, and lawful standards.

Reference 7 - 0.10% Coverage

America seeks an international system that lets nations pursue their interests peacefully, especially when those interests diverge; a system where the universal rights of human beings are respected, and violations of those rights are opposed; a system where we hold ourselves to the same standards that we apply to other nations, with clear rights and responsibilities for all.”

Reference 8 - 0.04% Coverage

These efforts require strong multilateral cooperation, enhanced domain awareness and monitoring, and the strengthening of international norms and standards.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 12 references coded [ 1.93% Coverage]

Reference 1 - 0.17% 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, recognizing our global responsibilities, as well as our national needs~

Reference 2 - 0.14% Coverage

The best engineers work together internationally to develop new standards for information systems that make networks faster and more reliable, catalyzing innovation and expanding accessibility~

Reference 3 - 0.18% Coverage

The collaborative development of consensus-based international standards for information and communication technology is a key part of preserving openness and interoperability, growing our digital economies, and moving our societies forward~

Reference 4 - 0.12% Coverage

Vulnerability reduction will require robust technical standards and solutions, effective incident management, trustworthy hardware and software, and secure supply chains~

Reference 5 - 0.18% Coverage

Likewise, in designing the next generation of these systems, we must advance the common interest by supporting the soundest technical standards and governance structures, rather than those that will simply enhance national prestige or political control~

Reference 6 - 0.05% Coverage

Economy: Promoting International Standards and Innovative, Open Markets

Reference 7 - 0.11% Coverage

Competition in these markets drives innovation, while a free-trade environment enables manufacturers to keep prices competitive and standards high~

Reference 8 - 0.17% Coverage

Respecting the international standards of technology development and trade is an essential part of sustaining open markets, and enables leading-edge technology companies to rapidly deliver the benefits of their innovative products and services

Reference 9 - 0.42% Coverage

Ensure the primacy of interoperable and secure technical standards, determined by technical experts. Developing international, voluntary, consensus-based cybersecurity standards and deploying products, processes, and services based upon such standards are the basis of an interoperable, secure and resilient global infrastructure~ 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 10 - 0.09% Coverage

International cybersecurity standardization, and its voluntary and consensus-based processes, serves collective interests~

Reference 11 - 0.13% Coverage

The United States will foster collaboration between the public and private sector to ensure the promulgation of international standards-based requirements for products and services~

Reference 12 - 0.16% Coverage

The United States will continue to identify, develop, and refine best practices and technical standards in collaboration and close partnership with industry, and will expand our efforts to promote awareness of and access to them~

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 DoD Cyber Strategy Summary - § 1 reference coded [ 0.85% Coverage]

Reference 1 - 0.85% Coverage

As the Sector Specific Agency (SSA) for the DIB and a business partner with the DIB and DCI, the Department will: set and enforce standards for cybersecurity, resilience, and reporting; and be prepared, when requested and authorized, to provide direct assistance, including on non-DoD networks, prior to, during, and after an incident.

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.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 7 references coded [ 0.65% Coverage]

Reference 1 - 0.11% Coverage

The revitalized Quad, which brings the United States together with Japan, India, and Australia, addresses regional challenges and has demonstrated its ability to deliver for the Indo-Pacific, combating COVID-19 and climate change, to deepening cybersecurity partnerships and promoting high standards for infrastructure and health security.

Reference 2 - 0.11% Coverage

Across our development work, we will continue to employ best practices that distinguish the United States and our partners from our competitors: transparency and accountability; high environmental, social, labor, and inclusion standards; respect for human rights; and local partnerships supported by foreign assistance and sound, sustainable financing.

Reference 3 - 0.09% Coverage

Therefore, as we engage globally and through international institutions, we will also deepen our cooperation with like-minded states to push for reforms on pandemic preparedness and if necessary to work more closely together to set higher standards that others can emulate.

Reference 4 - 0.05% Coverage

Since 1945, the United States has led the creation of institutions, norms, and standards to govern international trade and investment, economic policy, and technology.

Reference 5 - 0.10% Coverage

We are already rallying like-minded actors to advance an international technology ecosystem that protects the integrity of international standards development and promotes the free flow of data and ideas with trust, while protecting our security, privacy, and human rights, and enhancing our competitiveness.

Reference 6 - 0.11% Coverage

To ensure these investments support positive technological outcomes, we will partner with industry and governments in shaping technological standards that ensure quality, consumer safety, and global interoperability, and to advance the open and transparent standards process that has enabled innovation, growth, and interconnectivity for decades.

Reference 7 - 0.07% Coverage

We are working closely with allies and partners, such as the Quad, to define standards for critical infrastructure to rapidly improve our cyber resilience, and building collective capabilities to rapidly respond to attacks.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 DoD Cyber Strategy Summary - § 1 reference coded [ 0.27% Coverage]

Reference 1 - 0.27% Coverage

The Department will support whole-of-Government efforts to raise U.S. cybersecurity standards in order to increase resilience and make it more difficult for adversaries to disrupt these essential services.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 11 references coded [ 1.35% Coverage]

Reference 1 - 0.06% Coverage

Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance

Reference 2 - 0.10% Coverage

By leveraging existing international standards in a manner consistent with current policy and law, regulatory agencies can minimize the burden of unique requirements and reduce the need for regulatory harmonization.

Reference 3 - 0.10% Coverage

Our approach will also include targeting the illicit cryptocurrency exchanges on which ransomware operators rely and improving international implementation of standards for combatting virtual asset illicit finance.

Reference 4 - 0.11% Coverage

The CRI has gained the commitment of members to implement international AML/CFT standards, including know-your-customer (KYC) rules, to make it harder for ransomware actors to launder cryptocurrency proceeds from attacks.

Reference 5 - 0.15% Coverage

Over the long term, the United States will support implementation of international AML/CFT standards globally to mitigate the use of cryptocurrencies for illicit activities that undermine our national interest as part of our efforts to implement EO 14067, “Ensuring Responsible Development of Digital Assets.”

Reference 6 - 0.07% Coverage

This legislation should also set national requirements to secure personal data consistent with standards and guidelines developed by NIST.

Reference 7 - 0.11% Coverage

Any such legislation should prevent manufacturers and software publishers with market power from fully disclaiming liability by contract, and establish higher standards of care for software in specific high-risk scenarios.

Reference 8 - 0.12% Coverage

To begin to shape standards of care for secure software development, the Administration will drive the development of an adaptable safe harbor framework to shield from liability companies that securely develop and maintain their software products and services.

Reference 9 - 0.13% Coverage

Preserving and extending the open, free, global, interoperable, reliable, and secure Internet requires sustained engagement in standards development processes to instill our values and ensure that technical standards produce technologies that are more secure and resilient.

Reference 10 - 0.17% Coverage

United States and its foreign and private sector partners will implement a multi-pronged strategy to preserve technical excellence, protect our security, drive economic competitiveness, promote digital trade, and ensure that the “rules of the road” for technology standards favor principles of transparency, openness, consensus, relevance, and coherence.

Reference 11 - 0.24% Coverage

The Indo-Pacific Economic Framework for Prosperity (IPEF) and the Americas Partnership for Economic Prosperity (APEP) create opportunities for the United States and regional governments to collaborate in setting rules of the road for the digital economy, including facilitating the development of technical standards, mechanisms to enable cross-border data flows that protect privacy while avoiding strict data localization requirements, and actions to foster supply chain security and resilience.