Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 DoD Cyber Strategy - § 1 reference coded [ 0.21% Coverage]

Reference 1 - 0.21% Coverage

Public-private partnerships will necessarily require a balance between   
regulation and volunteerism, and they will be built on innovation, openness, and trust.

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 International Strategy for Cyberspace - § 10 references coded [ 1.23% Coverage]

Reference 1 - 0.13% Coverage

At the same time, our networks must be secure and reliable; they must retain the trust of individuals, businesses and governments, and should be resilient to arbitrary or malicious disruption~

Reference 2 - 0.14% Coverage

Computers can communicate with one another across a seamless landscape of global networks permitting trusted, instantaneous communication with friends and colleagues down the block or around the world~

Reference 3 - 0.06% Coverage

For cyberspace as we know it to endure, our networked systems must retain our trust~

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 - 0.19% Coverage

Because the Internet’s core functionality relies on systems of trust (such as the Border Gateway Protocol), states need to recognize the international implications of their technical decisions, and act with respect for one another’s networks and the broader Internet

Reference 6 - 0.11% Coverage

They foster innovation; facilitate interoperability, security, and resiliency; improve trust in online transactions; and spur competition in global markets~

Reference 7 - 0.12% Coverage

The United States Government actively participates in watch, warning, and incident response through exchanging information with trusted networks of international partners~

Reference 8 - 0.10% Coverage

The operation of critical networks and information infrastructures depends on the assured availability of trustworthy hardware and software~

Reference 9 - 0.09% Coverage

Protecting individual privacy is essential to maintaining the trust that sustains economic and social uses of the Internet~

Reference 10 - 0.15% Coverage

But connectivity is no end unto itself; it must be supported by a cyberspace that is open to innovation, interoperable the world over, secure enough to earn people’s trust, and reliable enough to support their work~

Files\\2011 Case Study\\CS1\_Primary Sources\_Policy\_Strategies\\2011 National Military Strategy - § 3 references coded [ 0.56% Coverage]

Reference 1 - 0.18% Coverage

Humanitarian assistance and disaster relief activities employ the Joint Force to address partner needs and sometimes provide opportunities to build confidence and trust between erstwhile adversaries.

Reference 2 - 0.19% Coverage

To shape the future force, we must grow leaders who can truly out-think and out innovate adversaries while gaining trust, understanding, and cooperation from our partners in an ever-more complex and dynamic environment.

Reference 3 - 0.19% Coverage

We will maintain the trust and confidence of our elected leaders and the public by providing frank, professional military advice; being good stewards of public resources; and vigorously executing lawful orders

Files\\2011 Case Study\\CS1\_Secondary Sources\_Authoritative\\2009 Cyberspace Policy Review Assuring a Trusted and R - § 4 references coded [ 0.04% Coverage]

Reference 1 - 0.03% Coverage

transparency and build trust between the civil liberties and privacy community, the public, and the program for cybersecurity,

Reference 2 - 0.01% Coverage

trust

Reference 3 - 0.01% Coverage

form trusted communities

Reference 4 - 0.01% Coverage

trusted

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 DoD Cyber Strategy - § 1 reference coded [ 0.09% Coverage]

Reference 1 - 0.09% Coverage

DoD will support U.S. government efforts to strengthen confidence-building measures to bring a greater level of trust to the U.S.-China relationship.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 National Military Strategy - § 3 references coded [ 0.35% Coverage]

Reference 1 - 0.07% Coverage

Operate on intent through trust, empowerment, and understanding

Reference 2 - 0.17% Coverage

To help us meet these goals, we are moving forward with a campaign of trust that stresses mutual respect and emphasizes the importance of a positive culture

Reference 3 - 0.10% Coverage

Such agreements allow us to strengthen the relationships that are the foundation of trust.

Files\\2015 Case Study\\CS2\_Primary Sources\_Policy\_Strategies\\2015 White House Report on Cyber Deterrence Policy - § 7 references coded [ 0.70% Coverage]

Reference 1 - 0.05% Coverage

trustworthiness of systems that support critical functions

Reference 2 - 0.04% Coverage

building and maintaining the public trust.

Reference 3 - 0.07% Coverage

Promoting Trust and Transparency in the International Community and Support for Partners

Reference 4 - 0.08% Coverage

the United States Government is pursuing bilateral and multilateral trust and transparency measures

Reference 5 - 0.14% Coverage

Trust is not only built through these strategic engagements, but also through day-to-day interaction and cooperation between the analysts who protect computer networks.

Reference 6 - 0.18% Coverage

Routine work, such as cooperation and information sharing between computer security incident response teams, builds relationships and trust that serve as an operational foundation for strategic trust and transparency.

Reference 7 - 0.14% Coverage

One example of such efforts is the United States Government’s collaboration with the private sector on implementing the National Strategy for Trusted Identities in Cyberspace

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2017 National Security Strategy - § 3 references coded [ 0.15% Coverage]

Reference 1 - 0.03% Coverage

Too many Americans had lost trust in our government, faith in our future, and confidence in our values.

Reference 2 - 0.04% Coverage

We will deny violent ideologies the space to take root by improving trust among law enforcement, the private sector, and American citizens.

Reference 3 - 0.08% Coverage

Relationships, developed over time, create trust and shared understanding that the United States calls upon when confronting security threats, responding to crises, and encouraging others to share the burden for tack l ing the world’s challenges.

Files\\2018 Case Study\\CS3\_Primary Sources\_Policy\_Strategies\\2018 DoD Cyber Strategy Summary - § 2 references coded [ 1.28% Coverage]

Reference 1 - 0.48% Coverage

Build trusted private sector partnerships: The private sector owns and operates the majority of U.S. infrastructure and is on the frontlines of nation-state competition in cyberspace.

Reference 2 - 0.81% Coverage

In coordination with other Federal departments and agencies, the Department will build trusted relationships with private sector entities that are critical enablers of military operations and carry out deliberate planning and collaborative training that enables mutually supporting cybersecurity activities.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Defense Strategy - § 1 reference coded [ 0.01% Coverage]

Reference 1 - 0.01% Coverage

We strive to be a trusted defense partner.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Military Strategy - § 1 reference coded [ 1.04% Coverage]

Reference 1 - 1.04% Coverage

7. STRENGTHEN RELATIONSHIPS WITH ALLIES AND PARTNERS Seek opportunities to collaborate and improve interoperability with allies and partners to confront enduring and emerging challenges. Foster strong relationships now — because we cannot surge trust in crisis.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2022 National Security Strategy - § 4 references coded [ 0.30% Coverage]

Reference 1 - 0.08% Coverage

We will seek greater strategic stability through measures that reduce the risk of unintended military escalation, enhance crisis communications, build mutual transparency, and ultimately engage Beijing on more formal arms control efforts.

Reference 2 - 0.06% Coverage

Around the world, we will increase cooperation and support to trusted partners, shifting from a strategy that is “U.S.-led, partner-enabled” to one that is “partner-led, U.S.-enabled.”

Reference 3 - 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 4 - 0.06% Coverage

Corruption also contributes to reduced public trust in state institutions, which in turn can add to the appeal of illiberal actors who exploit popular grievances for political advantage.

Files\\2023 Case Study\\CS4\_Primary Sources\_Policy\_Strategies\\2023 National Cybersecurity Strategy - § 5 references coded [ 0.45% Coverage]

Reference 1 - 0.14% Coverage

Malicious cyber activity has evolved from nuisance defacement, to espionage and intellectual   
property theft, to damaging attacks against critical infrastructure, to ransomware attacks and cyberenabled influence campaigns designed to undermine public trust in the foundation of our democracy.

Reference 2 - 0.07% Coverage

The American people must have confidence in the availability and resilience of this infrastructure and the essential services it provides.

Reference 3 - 0.06% Coverage

The American people must have confidence in the critical services underpinning their lives and the nation’s economy.

Reference 4 - 0.13% Coverage

Combining organizational collaboration and technologyenabled connectivity will create a trust-based “network of networks” that builds situational awareness and drives collective and synchronized action among the cyber defenders that protect our critical infrastructure.

Reference 5 - 0.06% Coverage

We will shift the consequences of poor cybersecurity away from the most vulnerable, making our digital ecosystem more worthy of trust.