Blueprint for a Secure Cyber Future

The Cybersecurity Strategy for the Homeland Security Enterprise

November 2011

Homeland Security

TABLE OF CONTENTS

MESSAGE FROM THE SECRETARY

I am pleased to release the *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*. This strategy was developed pursuant to the Department of Homeland Security (DHS) Quadrennial Homeland Security Review and reflects the importance of cyberspace to our economy, security, and way of life.

This strategy provides a blueprint for a cyberspace that enables innovation and prosperity, advances our economic interests and national security, and integrates privacy and civil liberties protections into the Department's cybersecurity activities. The strategy is designed to protect the critical systems and assets that are vital to the United States, and, over time, to foster stronger, more resilient information and communication technologies to enable government, business and individuals to be safer online.

Cybersecurity is a shared responsibility, and each of us has a role to play. Emerging cyber threats require the engagement of the entire society—from government and law enforcement to the private sector and most importantly, members of the public. Today in cyberspace, the Nation faces a myriad of threats from criminals, including individual hackers and organized criminal groups, as well as technologically advanced nation-states. Individuals and well-organized groups exploit technical vulnerabilities to steal American intellectual property, personal information, and financial data. The increasing number and sophistication of these incidents has the potential to impact our economic competitiveness and threaten the public's ability to access and obtain basic services. Government, non-governmental and private sector entities, as well as individuals, families, and communities must collaborate on ways to effectively reduce risk.

In preparing the strategy, the Department benefited from the constructive engagement of representatives from state and local governments, industry, academia, non-governmental organizations, and many dedicated individuals from across the country. We appreciate that support. DHS also worked closely with federal departments and agencies to refine the strategy and ensure consistency with the President's 2010 National Security Strategy, the Department of Defense Strategy for Operating in Cyberspace, and the President's International Strategy for Cyberspace.

I want to acknowledge the efforts and commitment of the men and women of DHS and the many thousands of computer scientists, systems engineers, law enforcement personnel, and other professionals across the country who work tirelessly to safeguard and secure cyberspace. On their behalf, I am pleased to release this *Blueprint for a Secure Cyber Future*.

Janet Napolitano

EXECUTIVE SUMMARY

The *Blueprint for a Secure Cyber Future* builds on the Department of Homeland Security Quadrennial Homeland Security Review Report's strategic framework by providing a clear path to create a safe, secure, and resilient cyber environment for the homeland security enterprise. With this guide, stakeholders at all levels of government, the private sector, and our international partners can work together to develop the cybersecurity capabilities that are key to our economy, national security, and public health and safety. The *Blueprint* describes two areas of action: Protecting our Critical Information Infrastructure Today and Building a Stronger Cyber Ecosystem for Tomorrow. The *Blueprint* is designed to protect our most vital systems and assets and, over time, drive fundamental change in the way people and devices work together to secure cyberspace. The integration of privacy and civil liberties protections into the Department's cybersecurity activities is fundamental to safeguarding and securing cyberspace.

The *Blueprint* lists four goals for protecting critical information infrastructure:

- Reduce Exposure to Cyber Risk
- Ensure Priority Response and Recovery
- Maintain Shared Situational Awareness
- Increase Resilience

These goals are supported by nine objectives. Each objective is dependent on a variety of capabilities that, when implemented, will work in tandem to effectively anticipate and respond to a wide range of threats. Some of the cybersecurity capabilities described in the *Blueprint* are robust and at work today, while others must be expanded. Still others require further research and development. All necessitate a collaborative and responsive cybersecurity community.

The *Blueprint* also lists four goals for strengthening the cyber ecosystem:

- Empower Individuals and Organizations to Operate Securely
- Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures
- Build Collaborative Communities
- Establish Transparent Processes

These goals are supported by eleven objectives, and depend on a broad set of capabilities, described in the Strategic Concept section of the *Blueprint*.

Achieving a safe, secure, and resilient cyber environment includes measuring progress in building capabilities and determining whether they are effective in an evolving threat environment. Accordingly, each year's performance will be compared with that of the previous year. This

approach will highlight where progress is being made and will identify gaps and resource requirements.

Cyberspace underpins almost every facet of American life, and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. Protecting cyberspace requires strong vision, leadership, and a broadly distributed effort in which all members of the homeland security enterprise take responsibility. The *Blueprint for a Secure Cyber Future* was developed to address this reality.

INTRODUCTION

The 2010 Quadrennial Homeland Security Review (QHSR)[1] established a strategic framework to guide the activities of the homeland security enterprise toward a common end: a homeland that is safe, secure, and resilient against terrorism and other hazards. To achieve this vision, the QHSR identified five core mission areas, and, in doing so, underscored the importance of cybersecurity to the Nation.

Homeland Security Mission Areas

1. Prevent Terrorism and Enhance Security
2. Secure and Manage our Borders
3. Enforce and Administer our Immigration Laws
4. **Safeguard and Secure Cyberspace**
5. Ensure Resilience to Disasters

These missions are the responsibility of the entire homeland security enterprise. Individuals across federal, state, local, tribal, and territorial governments, the private sector, and nongovernmental organizations are engaged in executing these missions. Beyond organizations such as the Department of Homeland Security (DHS) that are officially charged with the cybersecurity mission, responsibility begins with individual computer owners whose machines can be used in malicious attacks, and with the owners and operators of critical infrastructure systems. The roles and responsibilities across the homeland security enterprise for securing cyberspace reflect its size, diversity, and interdependent nature.

The creation of a mission area in the QHSR to safeguard and secure cyberspace builds on the President's National Security Strategy,[2] which:

- Declares the Nation's digital infrastructure a strategic national asset;
- Describes cyber threats as one of the most serious national security, public safety, and economic challenges we face as a Nation; and
- Requires that protection of digital infrastructure be a national security priority.

The Department of Homeland Security (DHS) has issued this *Blueprint for a Secure Cyber Future* (the *Blueprint*) to provide a clear plan of action for the homeland security enterprise to implement the National Security Strategy and achieve the goals set forth in the QHSR:

[1] http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf
[2] http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

- To Create a Safe, Secure, and Resilient Cyber Environment, and
- To Promote Cybersecurity Knowledge and Innovation.

The *Blueprint* has a single unifying concept: Protect Critical Information Infrastructure Today While Building a Stronger Cyber Ecosystem for Tomorrow. This strategic concept will drive prioritization of resources in order to systematically build the multiple capabilities needed to achieve QHSR Mission 4 goals. Appendix B provides a comprehensive mapping of the QHSR goals to the *Blueprint*.

Scope

Homeland Security Enterprise

Federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population. (Quadrennial Homeland Security Review Report 2010)

As set forth in the Homeland Security Act of 2002, [3] Homeland Security Presidential Directive (HSPD) 7: Critical Infrastructure Identification, Prioritization, and Protection,[4] National Security Presidential Directive (NSPD) 54/HSPD-23: Cybersecurity and Monitoring,[5] and Office of Management and Budget (OMB) guidance concerning implementation of the Federal Information Security Management Act of 2002 (FISMA),[6] DHS has the lead within the Federal Government to secure federal civilian executive branch information and communication systems,[7] to work with Sector-Specific Agencies and industry to protect privately-owned and operated critical infrastructure, and to work with State, local, tribal and territorial governments to secure their information systems. The roles of DHS and other federal departments and agencies in identifying, prioritizing, and protecting the Nation's critical infrastructure are described in statutes, Presidential directives, and documents such as the National Infrastructure Protection Plan (NIPP)[8] and the National Response Framework.[9] The Federal Government is, however, only one component of the homeland security enterprise, and successful implementation of this strategy requires the shared commitment of all stakeholders. In particular, cybersecurity is dependent on a strong two-way partnership between the public and private sector in areas such as information sharing, innovation, and implementation of best practices and standards.

Accordingly, the *Blueprint* is designed to give tangible and meaningful guidance to those in the homeland security enterprise who have a role in securing cyberspace and to benefit all who want to use information and communication technologies safely and securely as they go about their

---

[3] http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf
[4] http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm
[5] http://www.dhs.gov/xnews/releases/pr_1207684277498.shtm
[6] http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-28.pdf
[7] Although DHS receives information regarding vulnerabilities and incidents on DOD and other national security systems, the Department does not have the lead for securing these systems in the Federal enterprise.
[8] http://www.dhs.gov/files/programs/editorial_0827.shtm
[9] http://www.learningservices.us/pdf/emergency/nrf/nrp_cyberincidentannex.pdf

daily activities. Appendix C describes the strategy development process, including stakeholder outreach.

Relationship to Other Key Policies and Strategies

The *Blueprint* supports a whole-of-government approach to national security and is informed by current national cybersecurity strategy and policy as outlined in the following key documents: the White House Cyberspace Policy Review;[10] the President's International Strategy for Cyberspace;[11] the President's Strategy to Combat Transnational Organized Crime;[12] the Comprehensive National Cybersecurity Initiative (CNCI);[13] HSPD-7;[14] NSPD 54/HSPD-23;[15] FISMA;[16] the National Strategy for Trusted Identities in Cyberspace;[17] and the Department of Defense Strategy for Operating in Cyberspace.[18]

Motivation

America is deeply reliant on cyberspace. It is the very backbone of modern society. However, the technologies that enrich our professional and personal lives also empower those who would disrupt or destroy our way of life. Safeguarding and securing cyberspace is a homeland security mission because the potential exists for wide-scale or high-consequence adverse cyber events, which could cause harm to critical functions and services across the public and private sectors and impact national security, economic vitality, and public health and safety.

As malicious actors are using increasingly sophisticated tools, techniques, and procedures, and the volume and velocity of cyber incidents across the homeland security enterprise continue to grow:

- Critical infrastructure must protect against and be resilient in the face of advanced and persistent breaches which could degrade or disrupt the basic services upon which we depend, and set the stage for more destructive attacks.
- Government agencies must guard against exploits which may remove or corrupt sensitive data and interfere with the delivery of essential mission services.

---

[10] http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[11] http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
[12] http://www.whitehouse.gov/administration/eop/nsc/transnational-crime
[13] http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[14] http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm
[15] http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative
[16] http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
[17] http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
[18] http://www.defense.gov/news/d20110714cyber.pdf

- Large corporations, small businesses, and nonprofit organizations face increasingly sophisticated intrusions targeting their intellectual property and personal information about their customers and clients.
- Consumers are routinely at risk of identity theft to obtain unauthorized access to personal information at numerous points on the Internet.

Strategic Assumptions

While we cannot predict what cyberspace will look like many years from now, the Nation must seek to understand the forces that are shaping the future of cyberspace in order to lead, influence, and adapt to change. Accordingly, this strategy is based on the following assumptions:

- The increasing volume and sophistication of cyber exploitation demands heightened situational awareness, secure implementation of technology, coordinated incident response, demonstrated resilience in critical functions, and a professionalized cybersecurity workforce that is dynamically managed.
- Deepening social, economic, and industrial dependence on information and communication technologies creates opportunities for greater productivity and innovation and increases the number of users, devices, content, and processes to be protected in cyberspace.

- Rich interconnectivity transcends geographic boundaries, necessitating strong international collaboration. The risks posed through cyberspace offer a fundamental shift to the Nation's potential vulnerability, one which requires the adaptation of existing security and deterrence paradigms to a new reality.
- The aggregation of data in the cloud, combined with distributed, remote management, poses additional security opportunities and challenges.
- Mobile technology can expose sensitive data and processes to threat actors.
- Differences in cyber risk and risk tolerance at the individual, organizational, and national levels suggest that one-size-fits-all security measures will be less effective than risk-based solutions that can be tailored, focus on outcomes and performance, leverage user's natural reactions, promote innovation, and are cost-effective.
- Globalization of the information and communication technology supply chain creates new opportunities for innovation and competition as well as greater exposure to risk.

THE FUTURE WE SEEK

Vision

> Our vision is a cyberspace that supports secure and resilient infrastructure, that enables innovation and prosperity, and that protects privacy and other civil liberties by design. It is one in which we can use cyberspace with confidence to advance our economic interests and maintain national security under all conditions.
>
> —*Quadrennial Homeland Security Review Report 2010*

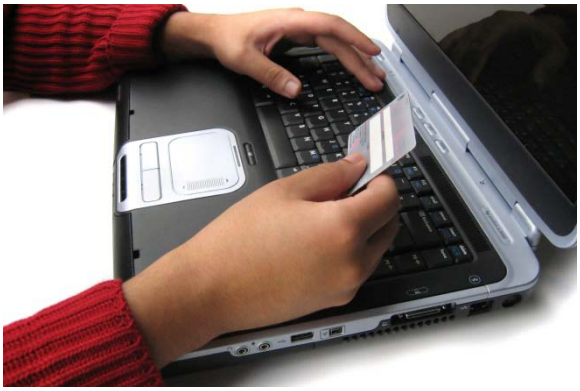
The information revolution has transformed nearly every aspect of daily life. A trusted digital infrastructure will provide a continued platform for innovation and prosperity and enable us to advance our economic and national security interests within an environment that upholds our core values. In order for future generations to realize the full potential of the information revolution, the homeland security enterprise must ensure safety, security, and resilience in cyberspace and promote cybersecurity knowledge and innovation. This complex, resource-intensive effort will require substantial research and development, along with ongoing operational refinement. The *Blueprint* provides a strong foundation for those efforts.

In keeping with the elements of the QHSR vision, the homeland security enterprise is committed to creating:

A Cyberspace that is Secure

Protecting the United States and its people, vital interests, and ways of life

In the future we seek, there will be major advances in securing cyberspace. Sensitive information will be protected by improved and innovative defenses. The American public will have confidence in their online transactions, and incidents affecting critical information infrastructure will be minimized. Individuals and organizations will be cognizant of threats and will rapidly adopt security measures that are consistent with them. Cybersecurity policy, regulation, and law, both domestically and internationally, will reflect the current cyber environment and anticipate future needs. Regulatory agencies will have the tools and staff needed to ensure that regulated entities implement appropriate security measures. Nation-states will be responsible parties in cyberspace and deny safe haven to those who would misuse the Internet. When cyberspace is used as an



attack vector or to commit crimes, agencies will have the necessary tools to identify the perpetrators and bring them to justice. Increased prosecutions will raise the costs of attacking or exploiting our information and communication systems. Federal agencies and private sector entities will have the technical cybersecurity workforce needed to meet their mission responsibilities.

A Cyberspace that is Resilient

Fostering individual, community, and system robustness, adaptability, and capacity for rapid response and recovery

In the future we seek, network architects will understand current and emerging threats and will design information and communication systems to cope with a range of contingencies; modeling, simulation, and exercises will enable the identification and mitigation of cascading impacts. Exercises will regularly test response and continuity plans to address the rapid restoration of critical functions and services, and to inform policy and investment decisions. The homeland security enterprise will have robust information sharing mechanisms – relevant knowledge about threats, vulnerabilities, and protective capabilities will be communicated in near real-time among people and devices in both the public and private sector. Critical operations will continue and network architectures will respond to unexpected events with agility.

A Cyberspace that Enables Innovation

Connecting people, devices, and markets to promote economic growth through collaborative innovation

In the future we seek, the American people will have ubiquitous access to cyber-enabled devices, enabling faster and more synergistic processes to support new levels of connectivity among individuals, businesses, and markets. Dialogue among previously isolated communities will continue to increase as users adopt novel ways of accessing information and services. New information and communication technologies will connect emerging markets with more prosperous markets, enabling growth in less developed areas as accelerated information transfer enables collaboration across diverse communities. Previously standalone devices, such as energy meters and home appliances, will be increasingly interoperable, allowing consumers and businesses to benefit from high efficiency. More robust security will reduce consumer risk and enable organizations to offer better service and increased capabilities online. Efforts to secure cyberspace will be undertaken in a manner that safeguards free trade and the broader free flow of information, recognizing our global responsibilities, as well as our national needs.

A Cyberspace that Protects Public Health and Safety

Ensuring the Safety of the American People

In the future we seek, industrial and supervisory control systems used to manage operations in critical infrastructure sectors such as Energy, Transportation, Water, Chemical, and Critical Manufacturing, and embedded systems used in medical devices, vehicles, and other industries, will be better protected from sabotage or attacks that could harm the general public. In addition, critical public safety functions, including law enforcement and emergency response services, will continue to rely on the availability and integrity of their information and communication technologies.

A Cyberspace that Advances Economic Interests and National Security

Enabling Economic Competitiveness and National Defense

In the future we seek, a safe, secure, and reliable cyberspace will fuel our domestic economy and the United States will remain a vibrant economic power. Businesses will have confidence in the confidentiality, integrity, and availability of their intellectual property and a better understanding of risks. A secure cyberspace will support the orderly functioning of the economy and delivery of essential services. A healthy cyber ecosystem will also facilitate performance of the other homeland security missions: prevention of terrorism; border security; enforcement of immigration laws; and resilience to disasters. And finally, through partnership with the Department of Defense (DOD), a secure cyberspace will support the United States' execution of its critical national defense mission responsibilities.

GUIDING PRINCIPLES

The *Blueprint* is guided by the values, principles, and way of life we expect as Americans. The protection of privacy and civil liberties is fundamental. The *Blueprint* also reflects the Administration's Open Government Initiative,[19] which calls for more transparent, participatory, and collaborative processes. Openness strengthens our democracy and promotes efficiency and effectiveness in government. Continued adherence to these principles will be key to continued stakeholder commitment to building out *Blueprint* capabilities.

Privacy and Civil Liberties

The homeland security enterprise will protect civil liberties and enhance privacy in our efforts to secure cyberspace. Individuals will be able to understand how their personal data may be used and be confident that it will be handled appropriately. We will support an open and interoperable cyberspace that enables individuals around the globe to seek, receive, and impart information and ideas. This free flow of information has proven essential to the rapid evolution and growth of the Internet. Cyberspace must continue to be a forum for free association and free speech.

Transparent Security Processes

The homeland security enterprise will implement security processes that have high levels of transparency and accountability. Adherence to the "need to share" and "responsibility to provide" collaboration principles will foster the transfer of specific, actionable cybersecurity information using approved methods to those who need it, while protecting the privacy and civil liberties of the public. Robust interaction among all levels of government, the private sector, and our international partners will enhance the effectiveness of security measures and improve the quality of decision making. All stakeholders will benefit from the exchange of information in a manner that supports both individual and collective interests and contributes to shared situational awareness.

Shared Responsibility in a Distributed Environment

Protective capabilities in cyberspace are naturally distributed across the homeland security enterprise, and considerable security expertise exists in many different areas. Accordingly, the homeland security enterprise will leverage the distributed nature of cyberspace in its own protection. We will work to strengthen local and individual capabilities, and to unite those capabilities in collective actions to realize shared security interests. To ensure cybersecurity for all of us, each of us must play a part. The homeland security enterprise will cultivate a sense of

[19] http://www.whitehouse.gov/open

shared responsibility and civic duty, and will use its combined knowledge to address security problems and drive action.

Risk-based, Cost Effective, and Usable Security

Security risks and tolerance for those risks vary across individuals, organizations, and at the national level. The homeland security enterprise must have a shared vision of what constitutes specific high-value systems and assets as well as the most important cybersecurity risks that must be mitigated. The enterprise will prioritize cybersecurity actions so that resources are consistently applied where they offer the greatest mitigation of risk. Effective mitigation of cyber vulnerabilities depends on a systematic accounting and broad awareness of risk, cost, and usability. All users take on some risks through the use of information and communication technologies. Users must have a greater understanding of those risks so they can make informed decisions about online behaviors and transactions.

STRATEGIC CONCEPT

A single, unifying strategic concept underpins the *Blueprint*: Protect Critical Information Infrastructure Today While Building a Stronger Cyber Ecosystem for Tomorrow. This strategic concept positions the Nation to achieve a safe, secure, and resilient cyberspace and shapes how stakeholders will work together to develop the capabilities needed for success.

Focus Areas

The strategic concept is composed of two complementary focus areas:

- The first focus area, "Protecting Critical Information Infrastructure," concentrates attention on systems and assets within the cyber ecosystem that are vital to the United States. This information infrastructure can best be protected by reducing exposure to risk, ensuring priority response and recovery, maintaining shared cyber situational awareness, and increasing resilience.

Critical Information Infrastructure

Any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice, or video that is:

- Vital to the functioning of critical infrastructure;
- So vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health and safety; or
- Owned or operated by or on behalf of a State, local, tribal, or territorial government entity. (Adapted from the Administration's cyber legislative proposal)

- The second focus area, "Strengthening the Cyber Ecosystem," is designed to drive fundamental change in the way people and devices work together to secure cyberspace. This evolutionary change in the computing environment will be achieved by empowering individuals and organizations to operate securely, making and using more trustworthy cyber protocols, products, services, configurations, and architectures, building collaborative communities, and establishing transparent processes.

Cyber Ecosystem

The cyber ecosystem is global and includes government and private sector information infrastructure, the variety of interacting persons, processes, information and communication technologies, and the conditions that influence their cybersecurity.

How the Focus Areas are Related

The two focus areas are interrelated and mutually supporting. Their interdependency can be seen, for example, in the development of the Nation's 21st century electric grid.

The "Smart Grid" will utilize an array of modern communications, sensing, control, and information technologies in order to:

- Modernize electricity generation, transmission, and distribution;
- Provide customers with actionable information so they can better understand their energy use and manage their electricity usage and bills more effectively; and
- Enable the widespread use of innovative technologies by consumers and industry.

Some of the components of the "Smart Grid" will be considered critical information infrastructure because their incapacity or destruction would be debilitating. Critical systems and assets may include power plants, electronic based transmission systems, smart transformers, and automated substations. Other components will be considered part of the broader cyber ecosystem: thermostats or appliances controlled by smart phones, plug-in electric vehicles, and rooftop solar panels.

While some components are more critical than others, the components drive one another and will work together to provide the Nation with a clean energy economy.

Defining Success

The capabilities described in the *Blueprint* are expected to provide measurable results that justify the investments being made across the homeland security enterprise. Anticipated results can be described within each focus area:

Protecting Critical Information Infrastructure

Critical information infrastructure[20] will be considered protected when outcome-based metrics demonstrate that owners and operators appropriately manage risks and the infrastructure is able to maintain adequate security, including confidentiality, integrity, and availability, in the face of the most consequential hazards.

Strengthening the Cyber Ecosystem

The ecosystem will be considered strong when the following conditions are met:

- Information and communication technology risk is well defined, understood and managed by users;
- Organizations and individuals routinely apply security and privacy standards and best practices;
- The identities of individuals, organizations, networks, services, and devices are appropriately validated;
- Interoperable security capabilities are built into information and communication technologies; and

[20] For the purpose of this strategy, Federal civilian executive branch information and communication systems as identified under the requirements of HSPD-7 are considered critical information infrastructure.

- Where appropriate, near real-time, machine-to-machine coordination provides indication, warning, and automated incident response.

How We Will Protect Critical Information Infrastructure

Protect Critical Information Infrastructure

- Reduce Exposure to Cyber Risk
- Ensure Priority Response and Recovery
- Maintain Shared Situational Awareness
- Increase Resilience

The security of the Nation's critical information infrastructure requires the interaction of multiple federal departments and agencies, as well as operational collaboration across federal, state, local, tribal, and territorial governments, nongovernmental organizations, and the private sector. In the Federal Government, cooperation between DHS and the military, intelligence, and law enforcement communities underpins our prevention and protection activities and our ability to respond effectively to incidents. The *Blueprint* describes how DHS will act under HSPD-7, NSPD-54/HSPD-23 and FISMA to take protective action with its partners and foster unity of effort. DHS will take a strong leadership role in protecting unclassified federal civilian executive branch systems and a lighter touch with the private sector.

Below, the *Blueprint* lists four goals for protecting critical information infrastructure, supported by nine objectives. The DHS role in achieving each objective is described in Appendix A. Each objective is dependent on a variety of capabilities that, when implemented, will work in tandem to effectively anticipate and respond to a wide range of threats. Some of the capabilities described below are robust and at work today while others must be expanded. Still others require further research and development. All necessitate a collaborative and responsive cybersecurity community.

Each capability is composed of people, processes, and enabling technologies that produce a discrete output. Because of the global nature of the cyber community, many of these capabilities will be developed and implemented in collaboration with our international partners. As stated in the Moving Forward section later in the *Blueprint*, prioritization of the capabilities will be described in a follow-on implementation plan.

DHS supports new legislation, developed as part of a broader Administration effort, which would facilitate the voluntary sharing of legally obtained cybersecurity information between the government and the private sector. Additionally, the proposal would provide liability protections to private sector entities for sharing cybersecurity information under the established guidelines. A legal context must be provided that encourages the appropriate, timely sharing of cybersecurity information between the government and private sector entities who are working toward a common goal.

Furthermore, the legislation would transparently, and with broad input from open public processes, grant or otherwise enhance the Department's authority to:

- Designate, for the purpose of increasing their cybersecurity, those entities that own or operate critical information infrastructure;[21]
- Identify specific cybersecurity risks that must be mitigated;
- Review and designate standardized frameworks to address these risks;
- Require entities to develop cybersecurity plans that identify the measures selected to address cybersecurity risks; and
- Establish third-party evaluation of the effectiveness of the entities in managing and mitigating cybersecurity risks.

DHS also supports legislation, developed as part of a broader Administration effort, which amends FISMA to give DHS primary responsibility within the federal civilian executive branch for information security.[22] This authority would allow DHS to:

- Issue compulsory policies and directives for information security and require implementation to govern agency information security operations;
- Review agency information security programs; and
- Designate an entity to receive reports and information about information security incidents, threats, and vulnerabilities affecting agency information systems.

These provisions, if enacted, would provide additional structure and oversight to the development of the core capabilities needed to achieve the goals and objectives listed below.

Reduce Exposure to Cyber Risk

1. **Avert Threats:** Decrease the ability of domestic and international criminals, including malicious insiders and foreign adversaries to exploit, impair, deny access to, or destroy critical information infrastructure, in part through the continued implementation of the Department's National Cybersecurity Protection System (NCPS).[23]

   Core capabilities[24] for the homeland security enterprise are:

---

[21] Subject to Congressional approval, entities would include specific companies from among the critical infrastructure sectors defined by HSPD-7.
[22] As stated in footnote seven on page two, DHS does not have the lead in securing DOD and other National Security Systems in the Federal enterprise.
[23] The capability to avert threats is dependent upon situational awareness, information fusion, and dissemination, as discussed in Objective Number 6 and Objective Number 7.
[24] *Presidential Policy Directive-8: National Preparedness* mandates the "development of a national preparedness goal that identifies the core capabilities necessary for preparedness" for the greatest threats to the Nation, including cyber attack. The National Preparedness Goal, released in September 2011, includes cybersecurity as a core capability to "[p]rotect against damage to, the unauthorized use of, and/or the exploitation of (and, if needed, the restoration of) electronic communications systems and services (and the information contained therein)." The implementation of the *Blueprint* will support the cybersecurity targets within the Protection Mission Area of the National Preparedness Goal. For further information on PPD-8, see

- Intrusion prevention systems (IPS) and other security technologies which minimize the amount of malicious traffic entering or exiting information and communication systems.
- Heightened domestic and international law enforcement activity to deter, investigate, and prosecute crimes committed through the use of cyberspace. Capacity will be increased through specialized technical training, use of advanced investigative and forensics tools, and development of productive international relationships to safeguard and share evidence and bring individuals to justice.
- Proactive identification of threat actors and tactics, techniques, and procedures through all-source information collection and analysis.
- Distribution of timely, specific, and actionable information on the most dangerous threats to critical information infrastructure. Information sharing forums, analysis centers, working groups, collaboration portals, briefings and other mechanisms facilitate the distribution and exchange of threat information with stakeholders across the homeland security enterprise.
- Creation of a community of interest that engages threat information producers and consumers with the goal of establishing standards for describing, interpreting, and automating threat information.
- Guidelines and incentives for incident reporting to the appropriate authorities, including organizational security professionals, State, local, tribal and territorial authorities, federal law enforcement, and incident response centers.

2. **Identify and Harden Critical Information Infrastructure:** Deploy appropriate security measures to manage risk to critical systems and assets.

   Core capabilities for the homeland security enterprise are:

   - Identification of those parts of the critical information infrastructure most likely to affect national security, national economic security, or national public health or safety if disrupted, damaged or destroyed including Internet peering points, the domain name system, satellite ground stations, cable landings, industrial and supervisory control systems, key business power or transportation systems, and other systems that support critical functions and services.
   - Management of networks through technical and operational guidelines.[25]
   - Assessment and prioritization of risk including the probability that a particular threat source will accidentally trigger or intentionally exploit a particular vulnerability and the

---

http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm For further information on the National Preparedness Goal, see http://www.fema.gov/pdf/prepared/npg.pdf

[25] One example is the National Security Agency Manageable Network Plan http://www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlan.pdf

resulting impact if this should occur. Risk assessments at the system, organizational, sector, regional, national, and international levels provide insights that enable public and private sector entities to prioritize mitigation actions and investments.

- Effective risk management using a framework of cybersecurity performance standards, including those adopted through voluntary codes of conduct within or across critical infrastructure sectors. Specific management, technical, and operational safeguards to reduce threat capabilities and vulnerabilities are included in voluntary consensus standards and federal publications.[26]
- Continuous monitoring and measurement of internal networks to ensure risk management actions are implemented and updated as appropriate for changes in technology or the threat environment. Third party review of risk management actions will validate that performance standards are being met.
- Standards-based automation to identify, classify and prioritize vulnerabilities and weaknesses in critical infrastructure technology.

3. **Pursue Operational, Architectural, and Technical Innovations**: Develop new ways to address existing problems and research solutions to counter emerging security challenges.[27]

   Core capabilities for the homeland security enterprise are:

   - Research and development (R&D) programs focused on key security priorities. The Federal Networking and Information Technology Research and Development (NITRD) Program has defined the following cybersecurity research and development themes that focus on game-changing technologies that can significantly enhance the trustworthiness of cyberspace: Designed-in Security, Tailored Trustworthy Spaces, Moving Target, and Cyber Economic Incentives.[28]
   - Rapid transition of products, tools, and capabilities from development to operation to match the dynamic nature of the threat through a pilot or test environment to assess the ability of the product to perform in the targeted architecture. Deployments of new technology must be supported by agile acquisition processes which match the technology development life cycle.
   - Integration of national cyber R&D activities, to include defense, law enforcement, counterintelligence, and homeland security directed research activities while ensuring the alignment of DHS-funded activity to secure critical infrastructures with CNCI-articulated research priorities and programs.

---

[26] One example is National Institute of Standards and Technology (NIST) Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

[27] The national R&D agenda for cybersecurity is defined and discussed in the DHS Roadmap for Cybersecurity Research. For additional discussion, see http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[28] For further discussion of these concepts, outlined in the NITRD Game-Change Research and Development Recommendations, see http://www.nitrd.gov/pubs/CSIA_IWG_%20Cybersecurity_%20GameChange_RD_%20Recommendations_20100513.pdf

Ensure Priority Response and Recovery

4. **Leverage the Enterprise in Taking Priority Actions**: Unify efforts to collaboratively respond to and rapidly recover from significant cyber incidents that threaten public health or safety, undermine public confidence, have a debilitating effect on the national economy, or diminish the security posture of the Nation.

   Core capabilities for the homeland security enterprise are:

   - Timely and accurate detection, reporting, analysis, and response when cyber incidents occur through watch and warning centers such as the National Cybersecurity and Communications Integration Center (NCCIC), which, together with component operations elements, collects and integrates information regarding cyber incidents and coordinates national response efforts with federal, state, local, tribal, and territorial government, private sector, and international partners.
   - Mature and well-exercised incident response and recovery plans which address both cyber incidents with physical consequences and physical incidents with cyber impacts. These include the National Cyber Incident Response Plan, the National Response Framework, and the National Incident Management System, as well as specific sector and organizational incident response plans.
   - Strong partnerships among homeland security enterprise stakeholders for rapid restoration of critical information infrastructure, including close coordination with first responders, and remote or onsite technical assistance by government or private sector subject matter experts as needed.
   - Cyber threat investigations and forensics analysis to determine the methods and paths of malicious activity, determine the impact to the infrastructure, provide evidence for prosecution, inform the development of other countermeasures, and offer predictive analysis to anticipate and help protect against future adversarial actions. The FBI-led National Cyber Investigative Joint Task Force (NCIJTF) is an interagency focal point for such cyber threat investigations and analysis. Its capabilities include reverse engineering attack vectors and attributing the digital and/or physical identity of the attacker.
   - Standards-based automated remediation capabilities to restore systems to known, secure states.

5. **Prepare for Contingencies:** Routinely conduct tabletop and functional exercises to test contingency plans and capture lessons learned.

   Core capabilities for the homeland security enterprise are:

   - Cross-sector exercises and simulations that work to assess and validate cross-sector cyber preparedness in areas such as information sharing, incident response, and incident recovery.

- Organization and sector-specific exercises which test processes, procedures, reporting mechanisms, information flows, and relationships necessary to respond to and recover from incidents at the system, organization, sector, regional, national, or international levels.
- Continuity planning, giving consideration to facilities, personnel, equipment, software, data files, and system components through the use of commercial backup sites, service-level agreements with hardware, software, and support vendors, and self-restoring services and systems (e.g., systems and communication traffic nodes that dynamically reroute traffic from the damaged nodes to the new and undamaged nodes).
- Mechanisms for assessing exercises, creating improvement plans, and codifying lessons learned in policies and procedures.

Maintain Shared Situational Awareness

Situational awareness is key to reducing exposure to risk, and ensuring priority response and recovery.

6. **Fuse Information:** Synthesize information developed through varied internal, local, national, and international sources.[29]

   Core capabilities for the homeland security enterprise are:

   - The NCPS, which is composed of people and sensors to collect and exchange information in real-time based upon specific stakeholder needs. Information needs are primarily focused on threat, vulnerability, consequences, warning, and countermeasures.
   - Analytic capacity through people, technology, and automated processes to rapidly correlate information from disparate sources. Results of the analysis will assist decision-makers at all levels and network security devices in preventing malicious activity. To this end, DHS, in collaboration with other departments and agencies is working to provide a common picture of relevant, operational cyber information to homeland security partners.
   - Information sharing with trusted partners, including peer and interdependent organizations, government agencies, and vendors through risk-mitigating fusion centers, sector-designated Information Sharing and Analysis Centers (ISACs), Sector Coordinating Councils, security and/or network operations centers, computer incident response teams, and consumers and suppliers in a supply chain.
   - Standardized agreements for collecting and accessing information in accordance with pre-defined processes, and for establishing a trusted sharing environment consistent with

[29] This objective has a dependency with Objective Number 1, Avert Threats and Objective Number 4, Leverage the Enterprise in Taking Priority Actions.

applicable law through memoranda of agreement/understanding, service-level agreements; contracts, and national-level regimes such as the Protected Critical Infrastructure Information (PCII) Program and the Chemical-Terrorism Vulnerability Information (CVI) designation which protect private sector information shared with the Federal Government.

7. **Distribute Information Efficiently:** Use multiple platforms to provide timely distribution of specific, actionable information.

   Core capabilities for the homeland security enterprise are:

   - Exchange timely cyber alerts developed by the U.S. Government with a wide range of stakeholders, through the development of systems such as United States Computer Emergency Readiness Team (US-CERT) Security Alerts and Bulletins, DOD cyber condition warnings, the FBI InfraGard program,[30] United States Secret Service Electronic Crimes Task Force network and the National Institute of Standards and Technology's National Vulnerability Database.
   - Robust processes for consistently disseminating accurate information related to threat signatures, indicators, vulnerabilities, and appropriate mitigations to relevant stakeholders in steady-state operations and during significant cyber incidents.
   - Effective communication strategies, including the use of social media, that meets desired objectives in terms of timeliness and frequency of communication, transmission and storage platforms, and communication risks.
   - Easy-to-use data portability measures which protect sources and methods and the originator of the information when necessary or make information accessible to wider audiences.
   - Economic incentives and direct assistance to strengthen collaboration through grants, subsidies, and tax credits, as well as consideration of liability protections.

8. **Provide Specialized and Continuing Security Training to the Cyber Workforce**: Collaborate to identify and deliver specialized cybersecurity training which improves workforce competency levels.

   Core capabilities for the homeland security enterprise are:

   - Improved training and education of technology professionals, allowing them to design, build and operate information technology systems that are fundamentally secure and resilient.

[30] http://www.infragard.net/

- A common body of knowledge for cybersecurity professionals. Knowledge can be increased via classroom-based and immersive learning environments as well as rotational assignments of personnel between the public and private sectors.
- Development and use of capability/skills maturity models for cybersecurity-related occupations and fields like Information Technology Management, Electronics Engineering, Computer Engineering, and Telecommunications. Capability maturity models describe the general and technical skills necessary to perform specific tasks at junior, intermediate, and senior levels.

Increase Resilience

9. **Increase System Fault Tolerance:** Be prepared to maintain critical operations in a degraded environment.

   Core capabilities for the homeland security enterprise are:

   - Comprehensive understanding of vulnerabilities, critical dependencies, and the potential for cascading disruptions on critical infrastructure.
   - Architectural guidance and standards for resilience, such as the reduction of single points of failure through multiple communications paths; storing a snapshot or "checkpoint" of an application in a known good state; fault isolation and containment; and reversion modes, in order to minimize disruption.
   - Conformance to established resilience standards and guidelines such as NIST Special Publication 800-34: *Contingency Planning Guide for Information Technology Systems* and International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27031:2011: *Information Technology Security Techniques – Guidelines for Information and Communications Technology Readiness for Continuity Planning*.
   - Methods to artificially and automatically create diversity in software systems and networks based upon the NITRD research program.[31]
   - Continuous audit of the effectiveness of resilience strategies and programs.

[31] http://www.cs.cornell.edu/fbs/publications/publicCYbersecDaed.pdf

How We Will Strengthen the Cyber Ecosystem

As described in the aforementioned smart grid example, critical information infrastructure exists within the broader cyber ecosystem. The homeland security enterprise will make phased improvements over time in the health of the cyber ecosystem, which will be achieved through empowered individuals and organizations; trustworthy protocols, products, services, configurations, and architectures; collaborative communities; and transparent processes. Below, the *Blueprint* lists four goals and eleven objectives within the broader effort to strengthen the cyber ecosystem.

Strengthen the Cyber Ecosystem

- Empower Individuals and Organizations to Operate Securely
- Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures
- Build Collaborative Communities
- Establish Transparent Processes

Empower Individuals and Organizations to Operate Securely

10. **Develop the Cyber Workforce in the Public and Private Sectors**: Maintain a strong cadre of cybersecurity professionals to design, operate, and research cyber technologies, enabling success against current and future threats.

    Core capabilities for the homeland security enterprise are:

    - Development of a rigorous cybersecurity and software assurance curriculum, and sustained enrollment in targeted fields of study. Relevant disciplines include science, technology, engineering, and math. The National Initiative for Cybersecurity Education (NICE) will strengthen formal cybersecurity education programs and use competitions to develop skill sets from kindergarten through 12th grade, and in higher education and vocational programs. Additionally, four-year colleges and graduate-level universities may apply to be designated as a National Center of Academic Excellence in Information Assurance Education.
    - Incentives for enrolling in targeted fields of study through scholarships, grants, subsidies, or tax incentives. The Federal Cyber Service: Scholarship for Service program provides scholarships that fully fund the typical costs that students pay for books, tuition, and room and board while attending an approved institution of higher learning.
    - Workforce retention. Techniques to build capacity include active recruiting, faster hiring, challenging assignments, structured career paths, and employee satisfaction surveys.
    - Preferred or required skills, including certification where appropriate, for cybersecurity professionals.

11. **Build a Base for Distributed Security**: Provide individuals with tools, tips, education, training, awareness, and other resources appropriate to their positions that enable them to

implement existing cybersecurity features and configurations in protocols, products, and services.

Core capabilities for the homeland security enterprise are:

- Cybersecurity awareness campaigns at the national, community, and organizational levels for specific segments of the population which provide users with tips, resources, and tools for recognizing cybersecurity challenges and doing their part in strengthening the ecosystem. These include DHS's "Stop.Think.Connect." campaign; the Cyber Awareness Coalition; Stay Safe Online; National Cyber Security Awareness Month activities at the federal, state, local, tribal and territorial levels; and individual organizational efforts to raise awareness among their workforce and stakeholders.
- Best practices and guidelines for actions individuals can take to strengthen their individual defenses and security posture.
- Mechanisms that notify users that their devices and systems have weaknesses or are infected, enabling them to take action.

Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations, and Architectures

12. **Reduce Vulnerabilities:** Design, build, and operate information and communication technology to specifically reduce the occurrence of exploitable weaknesses. Enable technology to sense, react to, and communicate changes in its security or its surroundings in a way that preserves or enhances its security posture.

    Core capabilities for the homeland security enterprise are:

    - Leadership in bodies and forums that develop international standards.
    - Widespread adoption of security-enabled software and hardware by end-users.
    - Guidelines and best practices for incorporating security into the system development lifecycle.
    - Security product evaluation or validation regimes.
    - Fundamental research to advance technology and drive the development of standards.
    - Innovation in the commercial market enabling the design of new technology to address emerging threats and attack attribution.
    - More agile acquisition processes that specify requirements for more trustworthy products and services and incorporate supply chain best practices that are competitive, timely, and promote innovation.

13. **Improve Usability**: Design trusted technology that is easy to use, easy to administer, rapidly customizable, and performs as expected.

    Core capabilities for the homeland security enterprise are:

    - Requirements and guidelines that indicate acceptable characteristics for assembly, configuration, operations administration, and performance such as the Human Computer Interface standards sponsored by the American National Standards Institute (ANSI) and UsabilityNet, an international project sponsored by the European Union.
    - Studies to determine the aspects of security technology which lead to rapid adoption and standardization within relevant user communities and should be characterized and integrated into the development process.

Build Collaborative Communities

Three capabilities—authentication, interoperability, and automation—are described in depth in the DHS white paper "Enabling Distributed Security in Cyberspace."[32]

14. **Appropriately Validate Identities in Cyberspace**: Use risk-based decision making for authentication, raising the level of trust associated with the identities of individuals, organizations, networks, services, and devices involved in online transactions and communication.

    Core capabilities for the homeland security enterprise are:

    - Authentication and authorization policies based on the risk and sensitivity of the activity being conducted through credential requirements, attribute/authorization requirements, remote access policies, and defined trust models.
    - Authentication and authorization best practices such as using attribute exchange and transactions, cryptographic logon, digital certificates, and other multi-factor authentication methods for high-risk or sensitive transactions.
    - Processes and design that can evolve with innovation like architecture, user-based design, policy-based routing and provisioning, correlating and de-conflicting policies, interoperability, and governance.

15. **Increase Technical and Policy Interoperability Across Devices:** On a device-to-device level, strengthen collaboration, create new intelligence, hasten learning, and improve situational awareness.

    Core capabilities for the homeland security enterprise are:

---

[32] http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

- A proven ability to communicate about cyber incidents through standardized dictionaries of key informational elements, including software vulnerabilities, weaknesses, patterns of attack, and malware classification as well as security content that is structured for automated sharing where appropriate. Resources include the National Vulnerability Database, Common Vulnerabilities and Exposures (CVE), and the Information Assurance Checklists housed on the National Checklist Program.[33]
- Interface standards to enable technical interoperability such as Public Key Cryptography Standards, Radio Frequency Identifier (RFID) air interface standards, and data format standards for the exchange of fingerprint, facial, or other biometric information.

16. **Automate Security Processes:** Employ automated mechanisms for acting collectively in near real-time to anticipate and prevent incidents, limit the spread of incidents across participating devices, and minimize consequences.

    - Digital policies that enable owners and operators to automate selected security actions in accordance with policy by taking infected devices offline where warranted, changing the configuration of healthy devices to harden them against intrusion, and blocking incoming malware and unauthorized outbound network traffic.
    - Collaboration frameworks and processes for defining and agreeing upon cybersecurity goals and collective courses of action that increase speed of action, optimize decision making, and ease adoption of new security solutions.

Establish Transparent Processes

17. **Publicize the Root Causes and Extent of Adverse Events in Cyberspace:** Widely share information on security hazards, analogous to how information about wellness and disease is reported by public health officials. Verify the location of incidents in existing and future top level domains (e.g., dot gov, dot com, and dot edu) and understand the causes, extent, and impact.

    Core capabilities for the homeland security enterprise are:

    - Information sharing mechanisms that enable the anonymized flow of incident data that is interoperable with current incident reporting services, such as those provided by the NCCIC and ISACs.
    - Information that is disseminated to homeland security enterprise stakeholders and international partners on cybersecurity capabilities and posture, hazards, and outbreaks that enable stakeholders to automatically execute preventative courses of action.

[33] http://checklists.nist.gov/

- Collaborative exploration of the threat environment through contributions from the Defense and Intelligence Community.

18. **Deploy Security Measures Based on Proven Effectiveness:** Share information about the security efficacy of cyber protocols, products, services, configurations, architectures, supply chains, and organizational processes.

    Core capabilities for the homeland security enterprise are:

    - Dissemination of information with homeland security enterprise stakeholders and international partners about the efficacy of cyber protocols, products, services, configurations, architectures, supply chains, and organizational processes in decreasing the spread and impact of hazards.
    - Mechanisms for prioritizing investments based on demonstrated results and ability to mitigate risk to acceptable levels.

19. **Focus on the Return on Investment**: Assess the organizational impact of cybersecurity investments on operating costs, capital budgets, business agility, and liability expenditures for data breaches or failure to meet service agreements.

    Core capabilities for the homeland security enterprise are:

    - Increase the speed of adoption and implementation of security measures by using methods to quantify the cost of cybersecurity investments and rapidly determine the resulting benefits of those investments.
    - Maintain and share data in order to demonstrate the costs and benefits of cybersecurity.

20. **Incentivize Performance:** Establish, maintain, and improve upon a system of goals and measures for cybersecurity.

    Core capabilities for the homeland security enterprise are:

    - Definition of goals and objectives, desired outcomes, and expected actions that enable the homeland security enterprise to articulate what success looks like.
    - Requirements, guidelines, policies, procedures, and voluntary codes of conduct that support homeland security enterprise goals and objectives.
    - Automated processes and mechanisms for collecting and displaying progress in meeting goals.
    - Analysis of efficiency, effectiveness and business/mission impact of cybersecurity measures, programs, and initiatives where resulting gaps inform efforts to redefine goals and objectives and make continuous improvements.

MOVING FORWARD

Cyberspace underpins almost every facet of American life and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. Protecting cyberspace requires strong vision, leadership, and a broadly distributed effort in which all members of the homeland security enterprise take responsibility. These collective efforts anticipate and reinforce a culture of teamwork and mutual accountability, recognition, and support.

This strategy articulates a clear path for meeting the vision of the National Security Strategy and achieving the goals set forth in the QHSR—creating a safe, secure, and resilient cyber environment and promoting cybersecurity knowledge and innovation. The two focus areas, "Protecting Critical Information Infrastructure" and "Strengthening the Cyber Ecosystem," will drive prioritization of homeland security enterprise capabilities, activities, and resources. Within DHS, this process will inform the Future Years Homeland Security Program, a five-year resource plan.

DHS will work with stakeholders in the homeland security enterprise to develop an implementation plan to prioritize activities, set milestones, and track progress in building the capabilities identified in the strategy. In addition, DHS will lead the homeland security enterprise in developing a mix of output and outcome metrics to measure the practical effectiveness of key security capabilities. DHS will work within the homeland security enterprise to establish baselines so that each year's performance can be compared with the previous year. This action will highlight where progress is being made, where gaps remain, and where additional resources are required. In meeting the demands of the cybersecurity mission, DHS will continue to protect privacy and civil liberties in accordance with applicable laws and principles.

Securing cyberspace is a complex endeavor that requires everyone's active participation. We are committed to making progress toward our goals by utilizing the inclusive framework provided by this strategy. Through these efforts, the homeland security enterprise can make cyberspace a safe, secure, and resilient place where the American way of life can thrive.

We welcome ongoing discussion of this strategy. Please contact us at cyberfeedback@dhs.gov to offer comments and suggestions.

APPENDIX A: ROLE OF DHS IN THE *BLUEPRINT*

Protect Critical Information Infrastructure

Goal: Reduce Exposure to Cyber Risk	
Objective	**Role of DHS**
1. Avert Threats	• Design, deploy, and operate (jointly with partners) the NCPS. • Conduct law enforcement investigations with other law enforcement entities. • Collect, analyze, and disseminate all-source intelligence with members of the Intelligence Community. • Distribute actionable information, including threat indicators. • Develop incident reporting guidelines. • With federal partners, maintain effective counterintelligence programs, including insider threat protections. • With federal partners, promote stronger domestic laws and enhanced international cooperation while protecting the privacy of individuals. • In coordination with the Department of State, collaborate and share best practices with international partners. • Sponsor research and development activities to identify and characterize malicious technology.
2. Identify and Harden Critical Information Infrastructure	• Lead, integrate, and coordinate the overall national effort to enhance critical infrastructure protection, including collaboratively developing the National Infrastructure Protection Plan and supporting Sector-Specific Plans. • Lead enterprise-wide efforts to secure federal civilian executive branch systems, including: continuous monitoring, sharing agency best practices, assessing the security of departments and agencies, advocating for the importance of effective technology management, helping agencies achieve cost savings for cybersecurity-related procurements, and developing enterprise-wide operational architectures and guidance. • Implement comprehensive, multi-tiered risk management programs and methodologies. • Recommend risk management and performance criteria and metrics within and across sectors. • Sponsor research and development activities and standards to automate the assessment of security risk. • Perform cybersecurity risk assessments, as appropriate.

Goal: Reduce Exposure to Cyber Risk	
Objective	**Role of DHS**
	• Incentivize adoption and use of security measures. • Serve as an example to other government agencies by implementing best practices and security measures on DHS information systems, networks, and data.
3. Pursue Operational, Architectural, and Technical Innovations	• Develop proactive approaches to improving security and managing cyber risk. • Transition products developed by research into operation on DHS systems and networks. • Support cybersecurity research efforts in coordination with government, private sector, and academic partners.

Goal: Ensure Priority Response and Recovery	
Objective	**Role of DHS**
4. Leverage the Enterprise in Taking Priority Actions	• Ensure a unified and coordinated response to significant cyber incidents. • Maintain the National Cyber Incident Response Plan. • Operate the NCCIC. • Integrate information from federal cybersecurity centers and other stakeholders to provide a common operating picture. • Conduct law enforcement and forensics investigations with other law enforcement entities. • Provide technical assistance in restoring critical information infrastructure.
5. Prepare for Contingencies	• Sponsor and facilitate national and international cross-sector exercises, focused on critical information infrastructure, and use lessons learned to inform best practices, policies, and procedures. • Maintain continuity plans for DHS systems and networks. • Partner with State, local, tribal, and territorial governments to improve incident response and recovery plans. • Work with stakeholders to prioritize cyber recovery efforts.

Goal: Maintain Shared Situational Awareness	
Objective	**Role of DHS**
6. Fuse Information	• Design, deploy, and operate (jointly with partners) the NCPS. • Analyze intrusions and incidents. • Provide stakeholders with a common operating picture. • Increase information sharing by working with stakeholders to

Goal: Maintain Shared Situational Awareness	
Objective	**Role of DHS**
	increase trust and reduce barriers (e.g., information sharing and handling agreements, use of tear lines to provide information at the lowest level of classification or restriction possible, private sector partnerships, and writing reports "for release").
7. Distribute Information Effectively	• Issue alerts regarding significant cyber threats, vulnerabilities, and incidents. • Use multiple platforms to promptly share actionable information with stakeholders. • Work to establish, refine, and maintain a trusted information sharing environment with increasing numbers of stakeholders.
8. Provide Specialized and Continuing Security Training to the Cyber Workforce	• Provide information and services, in collaboration with other federal partners, to enable the Nation's cybersecurity workforce to meet standards of competence.

Goal: Increase Resilience	
Objective	**Role of DHS**
9. Increase System Fault Tolerance	• Conduct vulnerability assessments of critical information infrastructure. • Promote the use of resilience standards and guidelines. • Sponsor research into high-assurance systems that are resistant to cyber intrusions.

Strengthen the Cyber Ecosystem

Goal: Empower Individuals and Organizations to Operate Securely	
Objective	**Role of DHS**
10. Develop the Cyber Workforce in the Public and Private Sectors	• Implement the National Initiative for Cybersecurity Education to raise awareness of risks among the American public, help develop the workforce structure, and recruit and train the next generation of the cybersecurity workforce. • Develop methods to generate interest in science, technology, engineering, and math programs in elementary school. • Promote cybersecurity career opportunities for students. • Support educational incentives.

Goal: Empower Individuals and Organizations to Operate Securely	
Objective	**Role of DHS**
	• Promote the use of workforce retention strategies by stakeholders. • Develop the DHS cyber workforce. • Become a model workplace for cybersecurity professionals.
11. Build a Base for Distributed Security	• Develop training and awareness materials. • Run the "Stop. Think. Connect." campaign. • Support other awareness campaigns by providing toolkits and additional information. • Make cybersecurity information and resources more readily available to the Nation's workforce. • Foster development of security tools for individual users.

Goal: Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures	
Objective	**Role of DHS**
12. Reduce Vulnerabilities	• Encourage innovation in the marketplace by purchasing commercial security products. • Coordinate the development of software assurance standards and benchmarking measures through public/private partnerships. • Encourage research and development. • Support the widespread use of trustworthy products. • Work with DOD and other research agencies to develop cybersecurity capabilities that support resiliency and reduce vulnerabilities across the government and the private sector. • Support the Department of Commerce's Internet Policy Task Force in developing the policies referenced in the Green Paper on Cybersecurity, Innovation and the Internet Economy.[34]
13. Improve Usability	• Encourage development of usability requirements and their incorporation into trusted technology. • Incorporate usability clauses into DHS contracts.

Goal: Build Collaborative Communities	
Objective	**Role of DHS**
14. Appropriately Validate Identities in Cyberspace	• Deploy multi-factor authentication to validate identities of DHS personnel. • Align DHS activities to the National Strategy for Trusted Identities in

[34] http://www.commerce.gov/sites/default/files/documents/2011/june/cybersecurity_green_paper_finalversion_0.pdf

Goal: Build Collaborative Communities	
Objective	**Role of DHS**
	Cyberspace (NSTIC), including further alignment with the Federal Identity, Credential, and Access Management (FICAM) Roadmap.[35] • Encourage stakeholder adoption of NSTIC. • Incentivize development of processes, technologies, and policies for managing online identities and how those identities can be used to access information resources.
15. Increase Technical and Policy Interoperability Across Devices	• Allocate resources to support the development and deployment of interoperable technologies, architectures, policies, and standards. • Encourage the public/private development of standardized dictionaries for security automation and measurement to facilitate information sharing and interoperability. • Build trust among stakeholders.
16. Automate Security Processes	• Work creatively and collaboratively with the private sector to define digital policies. • Support the development and piloting of automated security processes and frameworks.

Goal: Establish Transparent Processes	
Objective	**Role of DHS**
17. Publicize the Root Causes and Extent of Adverse Events in Cyberspace	• Enhance and promote methods for sharing information about the causes, extent and impact of hazards.
18. Deploy Security Measures Based on Proven Effectiveness	• Distribute information regarding proven strategies.
19. Focus on the Return on Investment	• Facilitate the sharing of business case information. • Enable the rapid transition of effective technologies from development to application across DHS and within critical infrastructure sectors.
20. Incentivize Performance	• Collaboratively build cybersecurity performance measures for the homeland security enterprise.

[35] For further information on NSTIC implementation, see http://www.nist.gov/nstic, for FICAM implementation and guidance, see http://www.idmanagement.gov and http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

APPENDIX B: MAPPING QHSR GOALS AND OBJECTIVES TO THE *BLUEPRINT*

The Quadrennial Homeland Security Review established high level goals and objectives for Mission 4, "Safeguard and Secure Cyberspace." These are:

> **Goal 4.1: Create a Safe, Secure, and Resilient Cyber Environment**. Ensure malicious actors are unable to effectively exploit cyberspace, impair its safe and secure use, or attack the Nation's digital infrastructure.
>
> **Objectives:**
>
> **Understand and prioritize cyber threats**. Identify and evaluate the most dangerous threats to federal civilian and private-sector networks and the Nation.
>
> **Manage risks in cyberspace**. Protect and make resilient information systems, networks, and personal and sensitive data.
>
> **Prevent cyber crime and other malicious uses of cyberspace**. Disrupt the criminal organizations and other malicious actors engaged in high-consequence or wide-scale cyber crime.
>
> **Develop a robust public-private cyber incident response capability**. Manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action.
>
> **Goal 4.2: Promote Cybersecurity Knowledge and Innovation.** Ensure that the Nation is prepared for the cyber threats and challenges of tomorrow.
>
> **Objectives:**
>
> **Enhance public awareness**. Ensure that the public recognizes cybersecurity challenges and is empowered to address them.
>
> **Foster a dynamic workforce**. Develop the national knowledge base and human capital capabilities to enable success against current and future threats.
>
> **Invest in innovative technologies, techniques, and procedures**. Create and enhance science, technology, governance mechanisms, and other elements necessary to sustain a safe, secure, and resilient cyber environment.
>
> —*Quadrennial Homeland Security Review Report* 2010

The two goals and their subordinate objectives provide baseline strategic guidance. The focal points "Protecting Critical Information Infrastructure" and "Strengthening the Cyber Ecosystem" are thematic organizing constructs which bring together the related QHSR objectives in a clear plan of action.

The following table maps the seven QHSR objectives to the *Blueprint*.

QHSR Objective	*Blueprint* Focus Area, Goal, and Objective
Understand and prioritize cyber threats. Identify and evaluate the most dangerous threats to federal civilian and private-sector networks and the Nation.	• Protecting Critical Information Infrastructure, Reduce Exposure to Cyber Risk, Avert Threats • Protecting Critical Information Infrastructure, Maintain Shared Situational Awareness, Fuse Information • Protecting Critical Information Infrastructure, Maintain Shared Situational Awareness, Distribute Information Efficiently
Manage risks in cyberspace. Protect and make resilient information systems, networks, and personal and sensitive data.	• Protecting Critical Information Infrastructure, Reduce Exposure to Cyber Risk, Identify and Harden Critical Information Infrastructure • Protecting Critical Information Infrastructure, Increase Resilience, Increase System Fault Tolerance • Strengthening the Cyber Ecosystem, Make and Use More Trustworthy Cyber Protocols, Reduce Vulnerabilities
Prevent cyber crime and other malicious uses of cyberspace. Disrupt the criminal organizations and other malicious actors engaged in high-consequence or wide-scale cyber crime.	• Protecting Critical Information Infrastructure, Reduce Exposure to Cyber Risk, Avert Threats • Strengthening the Cyber Ecosystem, Establish Transparent Processes, Publicize the Root Causes and Extent of Significant Cyber Incidents
Develop a robust public-private cyber incident response capability. Manage cyber incidents from identification to resolution in a rapid and replicable manner with prompt and appropriate action.	• Protecting Critical Information Infrastructure, Ensure Priority Response and Recovery, Leverage the Enterprise in Taking Priority Action • Strengthening the Cyber Ecosystem, Build Collaborative Communities, Automate Security Processes
Enhance public awareness. Ensure that the public recognizes cybersecurity challenges and is empowered to address them.	• Strengthening the Cyber Ecosystem, Empower Individuals and Organizations to Operate Securely, Build a Base for Distributed Security.
Foster a dynamic workforce. Develop the national knowledge base and human capital capabilities to enable success against current and future threats**.**	• Strengthening the Cyber Ecosystem, Empower Individuals and Organizations to Operate Securely, Develop the Cyber Workforce in the Public and Private Sectors • Protect Critical Information Infrastructure, Maintain Shared Situational Awareness, Provide Specialized and Continuing Security Training to the Cyber Workforce

QHSR Objective	*Blueprint* Focus Area, Goal, and Objective
Invest in innovative technologies, techniques, and procedures. Create and enhance science, technology, governance mechanisms, and other elements necessary to sustain a safe, secure, and resilient cyber environment.	• Strengthening the Cyber Ecosystem, Make and Use More Trustworthy Cyber Protocols, Products, Services, Configurations and Architectures, Reduce Vulnerabilities • Strengthening the Cyber Ecosystem, Build Collaborative Communities, Increase Technical and Policy Interoperability Across Devices • Strengthening the Cyber Ecosystem, Build Collaborative Communities, Automate Security Processes • Strengthening the Cyber Ecosystem, Build Collaborative Communities, Appropriately Validate Identities in Cyberspace • Protecting Critical Information Infrastructure, Reduce Exposure to Cyber Risk, Pursue Operational, Architectural, and Technical Innovations

APPENDIX C: STRATEGY DEVELOPMENT PROCESS

In developing the cybersecurity strategy for the homeland security enterprise, the Department has benefited from the constructive engagement of many organizations and individuals. Through a series of face to face meetings, webinars, conference calls, and e-mails, participants discussed a variety of topics, including strategic assumptions about the environment and strategic focus and approach.

Methodology

The strategy was developed with a focused methodology that emphasized close examination of the current and future strategic environment and consideration of alternative strategic concepts. Key elements of the methodology included:

- Assessment of the current strategic environment through analysis of key trends and dynamics.
- Exploration of the future strategic environment associated with cyberspace and cybersecurity.
- Examination of current policy, strategy, programs, and resource allocation across cybersecurity activities.
- Identification of key assumptions and associated policy implications.
- Consideration of alternative strategic concepts and analysis of priority ways and associated means to achieve our desired end-states efficiently and effectively.

The approach was executed through an inclusive and dynamic process anchored around an action officer study group and a senior-level steering committee.

Study Group: The study group was co-chaired by the National Protection and Programs Directorate (NPPD) Cyber Strategy Staff and staff from the Office of Policy, Office of Strategic Plans. The study group conducted analysis over an eight-month period, with work products shared with the other stakeholder groups via a variety of collaboration processes. The study group included members from many DHS components with support from subject-matter experts and research analysts from the Homeland Security Systems Engineering and Development Institute (HS SEDI) and the Homeland Security Studies and Analysis Institute (HSSAI), the Department's federally funded research and development centers.

Steering Committee: The steering committee was co-chaired by the Senior Counselor in NPPD and the Deputy Assistant Secretary for Policy. The steering committee met regularly with representatives from the study group and provided structured advice.

DHS Senior Leadership: Beginning with initial in-depth interviews, DHS senior leadership consistently provided guidance and decisions regarding scope, themes, and outputs. The study

group used the Department's forum for cybersecurity principals, the Cyber Jam, to socialize concepts.

Outreach

Congressional Engagement

The Department notified Congressional staff on the Homeland Security, Intelligence, and Defense committees at the outset of the strategy development process.

Other Federal Departments and Agencies

The Department worked with the following departments and agencies to develop the language contained in the strategy.

- Central Intelligence Agency
- Department of Commerce
- Department of Education
- Department of Energy
- Department of Defense
- Department of Health and Human Services
- Department of Justice
- Department of State
- Department of Transportation
- Department of the Treasury
- Environmental Protection Agency
- Federal Bureau of Investigation
- Federal Communications Commission
- General Services Administration
- National Security Agency
- Nuclear Regulatory Commission
- Office of the Director of National Intelligence
- Small Business Administration
- Social Security Administration

State, Local, Tribal, and Territorial and Private Sector Stakeholders

Early in the development of the *Blueprint*, DHS engaged multiple stakeholders, including members of the following public and private sector groups:

- The State, Local, Tribal, and Territorial Government Coordinating Council
- National Governors Association
- National Association of State Chief Information Officers
- Federal Senior Leadership Council
- Critical Infrastructure Cross-Sector Council
- Regional Consortium Coordinating Council
- Partnership for Critical Infrastructure Security
- National Council of Information Sharing and Analysis Centers
- Data Privacy and Integrity Advisory Committee
- Cross Sector Cyber Security Working Group
- Academia

DHS received detailed feedback as a result of our outreach from many group members. The study group carefully considered these comments as the strategy development effort proceeded.

APPENDIX D: GLOSSARY

Adequate Security	Security commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information being, processed, stored, or transmitted by information infrastructure. (Adapted from OMB Circular A-130)
Availability	The ability of information infrastructure to ensure timely and reliable access to the information it contains. (Adapted from 44 U.S.C. §3542)
Capability	A logically discrete grouping of people, processes, and enabling technologies that produces a discrete output: physical assets, information, relationships, transactions, or knowledge.
Cloud	A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. (CNSS Instruction 4009)
Common Operating Picture	The identical display of relevant, integrated information, based on common data, and available for viewing by interested and authorized parties.
Community	A body of individuals or organizations interacting in order to pursue mutual interests or goals. The traditional definition is of a geographically circumscribed entity such as a neighborhood or village, but common usage includes entities interacting without regard to physical, geographical, or political boundaries, for example, virtual communities, communities of practice, or the national community. Within the context of the cyber ecosystem, a community of organizations in a geographic region or an infrastructure sector might establish shared capabilities for understanding threats, assessing prevention options, reporting crime, or providing mutual assistance for response and recovery in the event of an incident. (Adapted from QHSR Appendix A)
Confidentiality	The ability of information infrastructure to preserve authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Adapted from 44 U.S.C. §3542)
Consequence	The effect of an event, incident, or occurrence. (DHS Risk Lexicon 2010)

Critical Information Infrastructure	Any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice or video that is: • Vital to the functioning of critical infrastructure; • So vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health or safety; or • Owned or operated by or on behalf of a State, local, tribal, or territorial government entity. (Adapted from the Administration's cyber legislative proposal)
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (42 U.S.C. §5195)
Critical Infrastructure Owner and Operator	Those entities responsible for day-to-day operation and investment in a particular asset or system. (National Infrastructure Protection Plan)
Cyber Ecosystem	The cyber ecosystem is global and includes government and private sector information infrastructure; the variety of interacting persons, processes, information, and communications technologies; and the conditions that influence their cybersecurity.
Cybersecurity	The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (NIPP)
Cyberspace	The interdependent network of information and communications technology infrastructures, including the Internet, telecommunications networks, computer systems and networks, and embedded processors and controllers in facilities and industries. (The White House Cyberspace Policy Review, May 2009)
Dot gov	For Internet addresses of the federal, state, and local governments as well as the Native Sovereign Nations, .gov is the top-level domain, except for the military which uses .mil.
Hazard	A natural or man-made source or cause of harm or difficulty. (DHS Risk Lexicon 2010)

Homeland Security Enterprise	Federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population. (QHSR 2010)
Information and Communication Technology	An umbrella term that includes information technology and any communication devices or applications, encompassing radio, television, cellular phones, computer and network hardware and software, satellite systems, and so on, as well as the various services and applications associated with them, such as videoconferencing and distance learning. (40 U.S.C. §1401)
Information Infrastructure	Any physical or virtual system or asset that controls, processes, transmits, receives, or stores electronic information in any form including data, voice or video.
Integrity	The ability of information infrastructure to guard against improper information modification or destruction, to ensure information non-repudiation and authenticity, and to ensure authenticity of information infrastructure components (e.g., network nodes or software applications). (Adapted from 44 U.S.C. §3542)
Intrusion	Unauthorized act of bypassing the security mechanisms of a system. (CNSS Instruction 4009)
Mitigation	Ongoing and sustained action to reduce the probability of or lessen the impact of an adverse incident. Includes solutions that contain or resolve risks through analysis of threat activity and vulnerability data, which provide timely and accurate responses to prevent attacks, reduce vulnerabilities, and fix systems. (NIPP)

National Security Systems	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— "(i) the function, operation, or use of which— (I) involves intelligence activities; (II) involves cryptologic activities related to national security; (III) involves command and control of military forces; (IV) involves equipment that is an integral part of a weapon or weapons system; or (V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications." (44 U.S.C. §3542)
Peering	Peering is a voluntary interconnection of administratively separate Internet networks for the purpose of exchanging traffic between the customers of each network.
Prevention	Actions taken and measures put in place for the continual assessment and readiness of necessary actions to reduce the risk of threats and vulnerabilities, to intervene and stop an occurrence, or to mitigate effects. (NIPP)
Private Sector	Organizations and entities that are not part of any governmental structure. The private sector includes for-profit and not-for-profit organizations, formal and informal structures, commerce, and industry. (National Response Framework)
Protection	Actions or measures taken to cover or shield from exposure, injury, or destruction. In the context of the NIPP, protection includes actions to deter the threat, mitigate the vulnerabilities, or minimize the consequences associated with a terrorist attack or other incident. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce surety, training and exercises, and implementing cybersecurity measures, among various others. (NIPP)

Recovery	The development, coordination, and execution of service- and site-restoration plans for affected communities and the reconstitution of government operations and services through individual, private sector, nongovernmental, and public assistance programs that identify needs and define resources; provide housing and promote restoration; address long-term care and treatment of affected persons; implement additional measures for community restoration; incorporate mitigation measures and techniques, as feasible; evaluate the incident to identify lessons learned; and develop initiatives to mitigate the effects of future incidents. (NIPP)
Resilience	The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption. (DHS Risk Lexicon 2010)
Response	Immediate actions to save lives, protect property and the environment, and meet basic human needs. Response also includes the execution of emergency plans and actions to support short-term recovery. (National Response Framework)
Risk	The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. Risk-based decision making is defined as the determination of a course of action predicated primarily on the assessment of risk and the expected impact of that course of action on that risk. (DHS Risk Lexicon 2010)
Sector	A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society. The NIPP addresses 18 critical infrastructure sectors, identified by the criteria set forth in HSPD-7.
Significant Cyber Incident	A Severe or Critical incident on the Cyber Risk Alert Level System. A Significant Cyber Incident is likely to cause, or is causing, harm to critical functions and services across the public and private sectors by impairing the confidentiality, integrity, or availability of electronic information, information systems, services, or networks; and/or threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation. Rapid identification, information exchange, investigation, response, and remediation often can mitigate the damage that a Significant Cyber Incident can cause and aid in rapid recovery and reconstitution after and during an incident. (National Cyber Incident Response Plan)

Situational Awareness	The set of timely cross-domain national-level information that will provide situational awareness on the state of U.S. cyber networks and systems to (1) know the availability, integrity, and confidentiality of U.S. cyber networks and systems, (2) understand the current and potential threats to U.S. cyber networks and systems, and (3) ensure that legitimate network operations are not mistaken for malicious activity.
Threat	A natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. (DHS Risk Lexicon 2010)
Trustworthy	For the purposes of this document, trustworthy is an umbrella term that encompasses safety, security, resiliency, reliability, privacy, and usability. See for example: http://www.nitrd.gov/fileupload/files/CSIAIWGCybersecurityGameChangeRDRecommendations20100513.pdf
Vulnerability	A physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard. (DHS Risk Lexicon 2010)

APPENDIX E: ACRONYM LIST

ANSI	American National Standards Institute
CNCI	Comprehensive National Cybersecurity Initiative
CVE	Common Vulnerabilities and Exposures
CVI	Chemical-Terrorism Vulnerability Information
DHS	Department of Homeland Security
DOD	Department of Defense
FBI	Federal Bureau of Investigation
FICAM	Federal Identity, Credential, and Access Management
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
HSSAI	Homeland Security Studies and Analysis Institute
HS SEDI	Homeland Security Systems Engineering Development Institute
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
NCCIC	National Cybersecurity and Communications Integration Center
NCIJTF	National Cyber Investigative Joint Task Force
NCPS	National Cybersecurity Protection System
NICE	National Initiative for Cybersecurity Education
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NITRD	Networking and Information Technology Research and Development Program
NPPD	National Protection and Programs Directorate

NSPD	National Security Presidential Directive
NSTIC	National Strategy for Trusted Identities in Cyberspace
OMB	Office of Management and Budget
PCII	Protected Critical Infrastructure Information
PPD	Presidential Policy Directive
QHSR	Quadrennial Homeland Security Review
R&D	Research and Development
RFID	Radio Frequency Identification
U.S.	United States
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team

Homeland
Security