U.S. DEPARTMENT OF HOMELAND SECURITY

CYBERSECURITY STRATEGY

May 15, 2018

Vision: *By 2023, the Department of Homeland Security will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities.*

TABLE OF CONTENTS

INTRODUCTION

The American people are increasingly dependent upon the Internet for daily conveniences, critical services, and economic prosperity. Substantial growth in Internet access and networked devices has facilitated widespread opportunities and innovation. This extraordinary level of connectivity, however, has also introduced progressively greater cyber risks for the United States. Long-standing threats are evolving as nation-states, terrorists, individual criminals, transnational criminal organizations, and other malicious actors move their activities into the digital world. Enabling the delivery of essential services—such as electricity, finance, transportation, water, and health care—through cyberspace also introduces new vulnerabilities and opens the door to potentially catastrophic consequences from cyber incidents. The growing number of Internet-connected devices and reliance on global supply chains further complicates the national and international risk picture. More than ever, cybersecurity is a matter of homeland security and one of the core missions of the U.S. Department of Homeland Security (DHS).

At DHS, we believe that cyberspace can be secure and resilient.[1] We work every day across the Department and with key partners and stakeholders to identify and manage national cybersecurity risks. We do this by adopting a holistic risk management approach. Like every organization, no matter how big or small, we must minimize our organizational vulnerability to malicious cyber activity by protecting our own networks. DHS also has broader responsibilities to protect the larger federal enterprise and improve the security and resilience of other critical systems. At the same time, we seek to reduce cyber threats by preventing and disrupting cyber crimes, and to lessen the consequences of cyber incidents by ensuring an effective federal response when appropriate. Finally, we work to create conditions for more effective cyber risk management through efforts to make the cyber ecosystem more fundamentally secure and resilient. This strategy sets forth our goals, objectives, and priorities to successfully execute the full range of the Secretary of Homeland Security's cybersecurity responsibilities.

Scope

This strategy provides the Department with a framework to execute our cybersecurity responsibilities during the next five years to keep pace with the evolving cyber risk landscape by reducing vulnerabilities and building resilience; countering malicious actors in cyberspace; responding to incidents; and making the cyber ecosystem more secure and resilient.

[1] The term "cyberspace" in this strategy refers to the interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computers, information and communications systems, and embedded processors and controllers.

The Cyber Threat

During the last several decades, advances in technology have fundamentally changed the world. Substantial growth in Internet access, use of Internet-enabled devices, and the availability of high speed information technology systems and large datasets have facilitated productivity, efficiencies, and capabilities across all major industries. The proliferation of technology also presents new cybersecurity challenges and leads to significant national risks. More than 20 billion devices are expected to be connected to the Internet by 2020. The risks introduced by the growing number and variety of such devices are substantial.

The United States faces threats from a growing set of sophisticated malicious actors who seek to exploit cyberspace. Motivations include espionage, political and ideological interests, and financial gain. Nation-states continue to present a considerable cyber threat. But non-state actors are emerging with capabilities that match those of sophisticated nation-states. Criminal actors are increasingly empowered by modern information and communications technologies that enable them to grow in sophistication and transnational reach. Transnational criminal organizations also increasingly collaborate through cyberspace. Complicating the threat picture, nation-states are increasingly using proxies and other techniques that blur the distinction between state and non-state cyber activities. In a number of cases, malicious actors engaged in significant criminal cyber activity appear to have both criminal and nation-state affiliations.

These diverse threats can impact federal and nonfederal information systems. Attempted incursions into government networks occur on a daily basis; the number of cyber incidents on federal systems reported to DHS increased more than ten-fold between 2006 and 2015. In 2015, a high-profile intrusion into a single federal agency resulted in the compromise of personnel records of over 4 million federal employees and ultimately affected nearly 22 million people. The growing interconnection of cyber and physical systems within critical infrastructure also creates the potential risk for malicious cyber activity to result in direct physical consequences; for example, the December 2015 overriding of controls in the Ukrainian electric grid resulted in widespread loss of power. Ransomware incidents such as WannaCry and NotPetya demonstrate how the rapid growth of the internet-of-things further complicates the threat as everyday devices can be targeted by malicious cyber actors with potentially far-reaching consequences.

The broad availability, relatively low cost, and increasing capabilities of cyber tools also affect trends in the threats we face. Ransomware, for example, has evolved to attack both frontline systems and backup drives. Malicious cyber actors have successfully used ransomware to compromise maritime, travel control, and healthcare systems. The Darkweb facilitates the easy sale of illicit goods and services, such as firearms, forged passports, and malware, which threat actors may acquire and use. Malware kits and instructions are also readily available on the Darkweb. Malicious cyber tools sold on the Internet can be adapted to intrude into systems and otherwise commit criminal acts related to financial fraud, money laundering, intellectual property theft, or other illicit activities. The growing popularity of cryptocurrencies also presents challenges to countering money laundering and the work of law enforcement.

Managing National Cybersecurity Risk

DHS must find innovative ways to leverage our broad resources and capabilities across the Department and the homeland security enterprise to strategically manage national cybersecurity risks. We have accordingly identified five pillars of a DHS-wide risk management approach. Through our efforts to accomplish seven identified goals across these five pillars, we work to ensure the availability of critical national functions and to foster efficiency, innovation, trustworthy communication, and economic prosperity in ways consistent with our national values and that protect privacy and civil liberties.

DHS Cybersecurity Goals

Pillar I – Risk Identification

- **Goal 1: Assess Evolving Cybersecurity Risks.** *We will understand the evolving national cybersecurity risk posture to inform and prioritize risk management activities.*

Pillar II – Vulnerability Reduction

- **Goal 2: Protect Federal Government Information Systems**. *We will reduce vulnerabilities of federal agencies to ensure they achieve an adequate level of cybersecurity.*

- **Goal 3: Protect Critical Infrastructure.** *We will partner with key stakeholders to ensure that national cybersecurity risks are adequately managed.*

Pillar III – Threat Reduction

- **Goal 4: Prevent and Disrupt Criminal Use of Cyberspace.** *We will reduce cyber threats by countering transnational criminal organizations and sophisticated cyber criminals.*

Pillar IV – Consequence Mitigation

- **Goal 5: Respond Effectively to Cyber Incidents**. *We will minimize consequences from potentially significant cyber incidents through coordinated community-wide response efforts.*

Pillar V – Enable Cybersecurity Outcomes

- **Goal 6: Strengthen the Security and Reliability of the Cyber Ecosystem**. *We will support policies and activities that enable improved global cybersecurity risk management.*

- **Goal 7: Improve Management of DHS Cybersecurity Activities.** *We will execute our departmental cybersecurity efforts in an integrated and prioritized way.*

The first pillar of our approach is better understanding our national risk posture. Understanding these risks at the strategic level will enable us to effectively allocate resources and prioritize efforts to address vulnerabilities, threats, and consequences across all of our cybersecurity activities.

Under pillars two through four, we focus on reducing or mitigating vulnerabilities, threats, and the potential consequences from cybersecurity incidents. DHS leads national efforts to protect

federal information systems, critical infrastructure, and other systems that impact national security, public health and safety, and economic security. These protective efforts seek to reduce organizational and systemic vulnerability to malicious cyber activity and empower stakeholders to make informed risk management decisions and to improve their cybersecurity. At the same time, our law enforcement Components work closely with each other, and throughout the law enforcement community, to reduce threats by aggressively investigating, disrupting, and defeating criminal actors and organizations that use cyberspace to carry out their illicit activities. To mitigate the consequences of cyber incidents, DHS draws upon its experience and capabilities in emergency management in addition to our network protection and law enforcement capabilities. DHS plays a lead role in the federal response to many cyber incidents, which may or may not involve physical consequences. DHS works with other federal agencies and stakeholders to minimize impacts and ensure that lessons learned from incidents are incorporated into future risk management efforts.

Finally, DHS also works to support cybersecurity risk management outcomes under the fifth pillar of our approach through efforts aimed at making cyberspace more defensible. This includes efforts to strengthen the security and reliability of the overall cyber ecosystem, and align our internal cybersecurity efforts. In particular, DHS seeks to foster security innovations that give an advantage to those protecting networks, and also to drive research, development, and technology transfer efforts. Because cyberspace is inherently global, DHS collaborates with the international community to build capacity, advocate for best practices, and promote responsible international behavior to ensure that the Internet remains open, interoperable, secure, and reliable. DHS also prioritizes efforts to address cybersecurity workforce challenges and empower organizations to recruit, hire, develop, and retain personnel with strong and enduring cybersecurity skillsets.

Through these complementary efforts across our Components, DHS works to collectively shift the advantage away from malicious cyber actors and toward those who are working to reduce national cybersecurity risks. Accomplishing our identified cybersecurity goals will also deter malicious cyber activity by denying access to, and imposing costs on, those who try to use cyberspace for illicit purposes. The cross-cutting goals and objectives set forth in this strategy are designed to ensure that DHS is maximizing its unique resources to accomplish impactful policy and operational outcomes as part of a national cybersecurity risk management approach.

Guiding Principles

DHS advances our mission and will accomplish our cybersecurity goals by aligning departmental activities according to the following guiding principles:

1. *Risk prioritization.* The foremost responsibility of DHS is to safeguard the American people and we must prioritize our efforts to focus on systemic risks and the greatest cybersecurity threats and vulnerabilities faced by the American people and our homeland.

2. *Cost-effectiveness*. Cyberspace is highly complex and DHS efforts to increase cybersecurity must be continuously evaluated and reprioritized to ensure the best results for investments made.

3. *Innovation and agility.* Cyberspace is an evolving domain with emergent risks. Although the proliferation of technology leads to new risks, it also provides an opportunity for innovation. DHS must lead by example in researching, developing, adapting, and employing cutting-edge cybersecurity capabilities and remain agile in its efforts to keep up with evolving threats and technologies.

4. *Collaboration.* The growth and development of the Internet has been primarily driven by the private sector and the security of cyberspace is an inherently cross-cutting challenge. To accomplish our cybersecurity goals, we must work in a collaborative manner across our Components and with other federal and nonfederal partners.

5. *Global approach.* Robust international engagement and collaboration is required to accomplish our national cybersecurity goals. DHS must engage internationally to manage global cyber risks, respond to worldwide incidents, and disrupt growing transnational cyber threats as well as encourage other nations and foreign entities to adopt the policies necessary to create an open, interoperable, secure, and reliable Internet.

6. *Balanced equities.* Cyberspace empowers people and enables prosperity worldwide. Cybersecurity is not an end unto itself, and efforts to mitigate cybersecurity risks must also support international commerce, strengthen international security, and foster free expression and innovation.

7. *National values.* DHS must uphold privacy, civil rights, and civil liberties in accordance with applicable law and policy. The Department empowers our cybersecurity programs to succeed by integrating privacy protections from the outset and employing a layered approach to privacy and civil liberties oversight.[2]

[2] See, for example, the Fair Information Practice Principles available at: https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

Development and Implementation

The DHS Office of Strategy, Policy, and Plans (PLCY) led the development of this strategy in collaboration with all DHS Components and in accordance with section 1912 of the 2017 National Defense Authorization Act.

In accordance with section 1912, DHS will also issue a corresponding implementation plan to outline Component roles, responsibilities, programs, and timelines for accomplishing these goals and objectives. This strategy and the implementation plan will be used to harmonize and prioritize DHS cybersecurity planning, programming, budget, training, and execution activities. In addition, the Joint Requirements Council will utilize the strategy and implementation plan to support the review of capability gap analyses and requirements generated by relevant Components. PLCY will annually assess implementation of this strategy and provide a report to the Secretary. The report will include areas of success, opportunities for improvement, constraints impeding progress, and suggested adjustments to the strategy. DHS will review and update this strategy in 2023, and periodically thereafter.

PILLAR 1 – RISK IDENTIFICATION

DHS must understand the global cybersecurity landscape and associated risks at the strategic level to effectively allocate our resources and prioritize departmental efforts to address vulnerabilities, threats, and consequences across all of our cybersecurity activities.

Goal 1: Assess Evolving Cybersecurity Risks

We will understand the evolving national cybersecurity risk posture to inform and prioritize risk management activities.

For DHS to effectively execute our mission in the long-term, we must work with stakeholders, including sector-specific agencies, nonfederal cybersecurity firms, and other federal and nonfederal entities, to gain an adequate understanding of the national cybersecurity risk posture, analyze evolving interdependencies and systemic risk, and assess changing techniques of malicious actors.

Objective 1.1: Maintain strategic awareness of trends in national and systemic cybersecurity risks.

Understanding trends in threats, vulnerabilities, interdependencies, and potential consequences over time will allow DHS to prioritize our protective, investigative, and response activities, and to plan and budget appropriately. DHS must also take stock of gaps in national analytic capabilities and risk management efforts to ensure a robust understanding of the effectiveness of cybersecurity efforts. We must anticipate the changes that future technological innovation will bring, ensure long-term preparedness, and prevent a "failure of imagination."

Sub-Objectives:

a. Identify evolving cybersecurity risks that affect national security, public health and safety, and economic security.
b. Identify and develop plans to address gaps in analytic capabilities and risk management efforts across DHS and national cybersecurity stakeholders.
c. Develop scenarios and plans for future technology developments and potentially disruptive innovations and adjust DHS efforts accordingly.

Outcomes:

DHS understands national and systemic cybersecurity risks and regularly adjusts our program and policy efforts to account for evolving technologies and operational priorities.

PILLAR II – VULNERABILITY REDUCTION

DHS works to reduce organizational and systemic vulnerabilities across the federal enterprise, including our own networks, as well as other nationally critical systems and assets. Through technical capabilities, cybersecurity information, and other assistance, we empower our stakeholders to better manage their cybersecurity risks.

Goal 2:
Protect Federal Government Information Systems

We will reduce vulnerabilities of federal agencies to ensure they achieve an adequate level of cybersecurity.

DHS leads the effort to secure the federal enterprise and must use all available mechanisms to ensure that every agency maintains an adequate level of cybersecurity, commensurate with its own risks and with those of the larger enterprise.[3] While individual agencies ultimately must implement their own cybersecurity risk-management programs because they are best positioned to understand their unique mission environments, DHS works with the Office of Management and Budget (OMB) to ensure an adequate level of security enterprise-wide and to address systemic risks and interdependencies across and between agencies. DHS must also support agency efforts to reduce their vulnerabilities to cyber threats by providing tailored capabilities, tools, and services to protect legacy systems as well as cloud and shared infrastructure. Within its own systems, DHS must continue to adopt new technologies and serve as a model for other agencies in the implementation of cybersecurity best practices.

In looking across the federal enterprise and in protecting its own information systems, DHS must address the greatest risks first and focus on the highest impact systems, assets, and capabilities. This means identifying the most critical systems and prioritizing protections around those systems. DHS must use cost-effective approaches that both get the most risk reduction leverage and ensure maximum return for investment. DHS must exhibit leadership through direct action and offerings, but also through collaboration with other agencies and stakeholders to pursue innovations like changes in federal information technology and procurement policies, improved analysis, and better operational planning. DHS must continue to closely collaborate with agencies including OMB, the U.S. General Services Administration, and the National Institute of Standards and Technology (NIST), as well as those responsible for protecting military and intelligence networks to deliver cybersecurity outcomes for the federal enterprise.

[3] DHS's authority to administer the implementation of agency information security policy and practices applies to systems of federal, executive-branch agencies, except for national security systems and certain Department of Defense and intelligence community systems. See 44 U.S.C. § 3553(b).

Objective 2.1: Increase cybersecurity of the federal enterprise through improved governance, information security policies, and oversight.

To execute our statutory responsibility to administer the implementation of agency information security policies and practices, DHS must continuously assess and advocate for changes to federal information technology governance structures and government-wide policies and programs that affect cybersecurity outcomes and investments. It is necessary to further refine and clarify roles and responsibilities between OMB, DHS, and other agencies. To start, DHS must provide better support to OMB's policy development and oversight role, and assess our own policies and programs to ensure efficiency and effectiveness. DHS must also advocate for and develop new processes to ensure accountability within agencies and across the federal enterprise in order to affect necessary cybersecurity changes. In support of these efforts, DHS must integrate information from existing protective capabilities along with relevant cybersecurity threat reporting from the intelligence community, law enforcement, and other sources to enhance the ability to understand individual agency, enterprise, and systemic risks, inform risk management decisions, and assess potential returns on investment. Driven by this information, the federal enterprise will be able to prioritize resources to meaningfully address policy and capability gaps and build a more modern, secure, and resilient information infrastructure.

Sub-Objectives:

a. Develop and implement a clear governance model for federal cybersecurity, including defining roles and responsibilities for legacy and cloud or shared services.
b. Issue new or revised policies and recommendations as required, consistent with DHS authorities, to ensure adequate cybersecurity across the federal enterprise.
c. Develop a formalized approach to measure and track agency adoption of information security policies, practices, and required controls.
d. Implement processes to increase agency accountability and compliance with information security policies, practices, and required controls.
e. Assess enterprise and individual agency risk posture through strategic analyses, available threat reporting, and other means to inform cybersecurity and investment priorities.
f. Provide agencies with integrated and operationally relevant information necessary to understand and manage their cyber risk.

Outcomes:

DHS-led efforts result in agencies maintaining an adequate level of cybersecurity, commensurate with each agency's risks and with those of the federal enterprise.

Objective 2.2: Provide protective capabilities, tools, and services across the federal enterprise.

DHS operates enterprise-wide capabilities and offers tools and services to assist agencies manage their cybersecurity risks. Certain elements of the federal enterprise must be further centralized to appropriately and consistently address key cybersecurity risks and provide improved enterprise-wide security. For example, DHS has made significant progress in establishing baseline protective capabilities across the federal enterprise through the deployment of perimeter security capabilities. DHS will establish additional capabilities to cost-effectively address key cybersecurity risks across the federal enterprise and to address increasing use of cloud infrastructure and shared services. DHS must also build on economic and operational efficiencies through the centralized purchase or in-house development of tools and services, where appropriate, to address threats to legacy systems and cloud or shared services. New tools and services may be offered to agencies on a reimbursable basis or without reimbursement when they provide needed capability to agencies, address priority threats, or are necessary to facilitate situational awareness, incident response, or other strategic goals.

Sub-Objectives:

a. Identify elements of the federal enterprise that should be centralized to cost-effectively address key cybersecurity risks and provide enterprise security.
b. Deploy, where appropriate, centralized protective capabilities to address enterprise-wide cybersecurity risk.
c. Develop and provide additional cybersecurity tools and services for agencies in response to emerging or identified threats.
d. Create performance metrics to measure the effectiveness of new and existing cybersecurity capabilities, tools, and services.

Outcomes:

Federal agencies utilize DHS capabilities, tools, and services to identify and mitigate cyber threats and vulnerabilities before they do significant harm.

Objective 2.3: Deploy innovative cybersecurity capabilities and practices to protect DHS information systems.

DHS must maintain an adequate level of security for our own systems. Many DHS information systems remain largely decentralized and are operated by Components without a standardized cybersecurity approach or methodology. DHS must undertake a systematic effort to assess our information systems at greatest risk, and to ensure that appropriate protective capabilities and methodologies are in place to secure sensitive information while enabling critical mission functions. DHS must adopt a more unified approach to securing our own information systems and, where appropriate, deploy standardized, cost-effective, and cutting-edge capabilities across high-value departmental information systems. As we increasingly leverage cloud and shared services, DHS must continue to develop and pilot emerging capabilities, tools, and practices to more effectively detect and mitigate evolving threats and vulnerabilities in a timely fashion and ensure that our cybersecurity approaches are flexible and dynamic enough to counter determined and creative adversaries. DHS must serve as a first adopter and model for other agencies as we work to modernize our information technology and the entire federal enterprise.

Sub-Objectives:

a. Conduct comprehensive risk and gap assessments across DHS information systems based on consistent methodology and government and industry best practices.
b. Deploy appropriate best-in-class technologies and practices, including standardized solutions where cost-effective and operationally feasible to secure legacy systems and cloud or shared services.
c. Pursue innovative and agile approaches to acquisition and technology procurement to deploy cutting-edge capabilities and facilitate use of cloud and shared services.
d. Pilot innovative capabilities, tools, and other new technologies or practices that can protect DHS systems and are potentially scalable across the federal enterprise level.

Outcomes:

DHS maintains an adequate level of cybersecurity, commensurate with our own risks and with those of the government-wide enterprise, to ensure the confidentiality, availability, and integrity of critical DHS information systems and information.

Goal 3:
Protect Critical Infrastructure

We will partner with key stakeholders to ensure that national cybersecurity risks are adequately managed.

DHS must ensure that growing cybersecurity risks across all critical infrastructure sectors and other systems that impact national security, public health and safety, and economic security are managed at an acceptable level.[4] DHS must partner with key stakeholders, including sector specific agencies and the private sector, to drive better cybersecurity by promoting the development and adoption of best practices and international standards, by providing services like risk assessments and other technical offerings, and by improving engagement efforts to advance cybersecurity risk management efforts. DHS must also expand operationally meaningful cybersecurity information sharing efforts to empower those protecting networks from cyber threats. To these ends, DHS serves an essential partnership role as the sector-specific lead or co-lead for 10 of the 16 critical infrastructure sectors and the Secretary coordinates the overall Federal effort to promote security and resilience across all of the sectors.[5] While continuing to leverage existing partnership structures, DHS must deepen technical collaboration across all the sectors and with other key nonfederal entities on risk mitigation efforts. As the agency

[4] Congress authorized DHS to engage broadly with federal and nonfederal entities to collaboratively address cybersecurity risks. See 6 U.S.C. § 148(c)(9).

[5] The 16 critical infrastructure sectors are: 1) Chemical; 2) Commercial Facilities; 3) Communications; 4) Critical Manufacturing; 5) Dams; 6) Defense Industrial Base; 7) Emergency Services; 8) Energy; 9) Financial Services; 10) Food and Agriculture; 11) Government Facilities; 12) Healthcare and Public Health; 13) Information Technology; 14) Nuclear Reactors, Materials, and Waste; 15) Transportation Systems; and 16) Water and Wastewater (*https://www.dhs.gov/critical-infrastructure-sectors*)

designated to lead the national effort to protect the Nation's infrastructure, DHS must also act as a backstop to ensure that cybersecurity threats do not disrupt the provision of essential services to the American people. DHS must, therefore, smartly leverage its regulatory authorities in tailored ways, and engage with other agencies to ensure that their policies and efforts are informed by cybersecurity risks and aligned to national objectives to address critical cybersecurity gaps.

To properly allocate resources and prioritize efforts, DHS must maintain substantial awareness of the cybersecurity risk posture across critical infrastructure. This includes understanding the potential consequences of infrastructure-related cybersecurity incidents. DHS must prioritize its engagement efforts based upon those with the highest risk, such as entities where a cyber incident could result in catastrophic impacts.[6]

Objective 3.1: Mature cybersecurity offerings and engagements to address significant national risks to critical infrastructure.

DHS must improve the cybersecurity of critical infrastructure through the development and deployment of tools, services, and other offerings, as well as through targeted outreach to critical infrastructure owners and operators, service providers, and other key enablers of risk management activity. DHS must routinely evaluate the value of these risk management efforts and assess capability gaps. In particular, DHS must engage sector-specific agencies, nonfederal cybersecurity firms, individual critical infrastructure entities, and other stakeholders to assess interdependencies and systemic risk across critical infrastructure, and identify gaps in risk management efforts. DHS offerings must be prioritized to focus on systemic risk or address risk at individual entities that have the greatest potential impact on national security, public health and safety, and economic security. Offerings that do not address identified gaps or provide DHS with access to unique cybersecurity information should be reconsidered.

To ensure effective outreach, DHS must take a disciplined approach to identify its key stakeholders, including entities across all 16 critical infrastructure sectors and key enablers of risk management activities. DHS must expand efforts to encourage adoption of applicable cybersecurity best practices, including NIST's *Framework for Improving Critical Infrastructure Cybersecurity*.[7] DHS must also increasingly leverage field personnel to engage geographically diverse stakeholders to encourage the adoption of cybersecurity risk management best practices and provide access to available cybersecurity information, risk management offerings, and other DHS-wide capabilities. DHS must also be prepared to engage with officials at the appropriate levels within an organization to ensure that gaps in critical infrastructure cybersecurity involving potentially significant impacts on national security, public health and safety, or economic security are addressed.

[6] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (2013), section 9 (*https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf*).
[7] Available at *https://www.nist.gov/cyberframework*.

Sub-Objectives:

a. Understand the interdependencies across critical infrastructure and systemic risks that affect national security, public health and safety, and economic security.
b. Evaluate the efficacy, quality, and usage of DHS cybersecurity risk management offerings provided to various critical infrastructure and other key stakeholders.
c. Assess impact of engagement by DHS personnel on progress toward adoption of best practices and usage of DHS offerings.
d. Identify and prioritize gaps in current national cybersecurity risk management efforts.
e. Address identified gaps through tools, services, and other offerings provided to critical infrastructure owners and operators or other key entities.
f. Establish mechanisms to mitigate persistent cybersecurity risks with a potential significant impact on national security, public health and safety, or economic security.

Outcomes:

DHS reduces the most significant national risks to critical infrastructure, especially those where incidents could have a significant impact on national security, public health and safety, and economic security.

Objective 3.2: Expand and improve sharing of cyber threat indicators, defensive measures, and other cybersecurity information.

DHS must assess and improve existing information sharing efforts to ensure that the most operationally useful information is provided to our stakeholders. We serve as the main federal interface for receiving and sharing cyber threat indicators and defensive measures between and among nonfederal entities and with other agencies.[8] DHS must build on and expand automated mechanisms to receive, analyze, and share cyber threat indicators, defensive measures, and other cybersecurity information with critical infrastructure and other key stakeholders. DHS must continue to pursue programs for sharing vulnerability information and classified cybersecurity information where appropriate, while also emphasizing the need to rapidly declassify cyber threat and associated contextual information. DHS must continue to partner with information sharing and analysis centers and other information sharing and analysis organizations to increase access to and collaboration regarding cybersecurity information. We must identify and address barriers to sharing information with the U.S. Government and between agencies. In addition to expanding its information sharing and collaboration capacities, DHS must improve its analytic capabilities to enhance the quantity and quality of information shared and increase the value of information sharing programs for all critical infrastructure stakeholders.

Sub-Objectives:

a. Continue to expand participation in information sharing programs and increase the cybersecurity information shared by all participants.
b. Support engagement with information sharing and analysis centers, information sharing and analysis organizations, and other information sharing entities or fora.
c. Increase the ability of DHS to analyze, correlate, and enrich data received and shared with all cybersecurity information sharing partners.

[8] The terms "cyber threat indicator" and "defensive measure" are defined in the Cybersecurity Information Sharing Act of 2015, at 6 U.S.C. § 1501.

d. Improve technical platforms and mechanisms to share cybersecurity information and collaborate with stakeholders, including in highly automated ways.
e. Evaluate the efficacy of, and continue to improve, DHS programs to share or access classified and unclassified U.S. Government information to protect nonfederal entities.

Outcomes:
Cybersecurity stakeholders increasingly leverage information shared by DHS to quickly understand cybersecurity risks and protect their information systems.

Objective 3.3: Improve cybersecurity capabilities and resources available to sector-specific agencies, regulators, and policymakers.

As a sector specific agency for 10 critical infrastructure sectors, DHS must ensure institutional knowledge and specialized expertise for each of these sectors in order to best support that sector during steady-state and incident response activities. In addition, DHS has regulatory authority with respect to chemical and transportation sectors. DHS must maintain relevant expertise, mature existing voluntary and regulatory partnerships, and continue to integrate cyber and physical resources for these sectors. DHS must also continue to mature our capabilities to provide non-DHS sector-specific agencies, regulators, and other policy-making entities with cybersecurity expertise to inform efforts to protect the Nation's critical infrastructure. DHS must leverage its expertise to shape the wide array of federal and nonfederal policies that can drive significant advancements in cybersecurity.

Sub-Objectives:
a. Enhance sector-specific cyber expertise to understand the potential impact of cyber incidents and facilitate risk management efforts.
b. Assess and update DHS policies and regulations to address cybersecurity risk to covered entities.
c. Support each critical infrastructure sector in developing and employing appropriate cybersecurity approaches and technical support mechanisms.
d. Identify and provide technical and other support to significant non-DHS regulatory and policy efforts that affect management of national cybersecurity risk.

Outcomes:
All of the 16 critical infrastructure sectors are aware of cyber risks to their sector and maintain sufficient cybersecurity-related policies and capabilities to support risk management efforts.

PILLAR III – THREAT REDUCTION

DHS law enforcement agencies investigate and reduce threats from cyber criminals. In partnership with other law enforcement agencies, DHS must prevent cyber crime and disrupt criminals and criminal organizations who use cyberspace to carry out their illicit activities and leverage identified threat activity and trends to inform national risk management efforts.

Goal 4:
Prevent and Disrupt Criminal Use of Cyberspace

We will reduce cyber threats by countering transnational criminal organizations and sophisticated cyber criminals.

Law enforcement performs a critical role in cybersecurity risk management by focusing on the threat, and preventing the use of cyberspace for illicit purposes. While breaches of sensitive personal information generate significant media attention, financial fraud, money laundering, theft of intellectual property and sensitive technologies, selling of illicit goods, and child exploitation are also increasingly being conducted online. In response, nearly all criminal investigations now require law enforcement investigators to have knowledge of computer forensics, digital investigations, and the cyber tradecraft that is necessary to counter transnational criminal threats. Improved criminal intelligence is also a key component of cyber investigations and combatting transnational criminal organizations.

DHS must continue to strengthen our efforts as part of the law enforcement community to pursue, counter, reduce, and disrupt illicit cyber activity by leveraging, in particular, our specialized expertise and capabilities to target financial and trans-border cyber crimes.[9] The transnational and cross-jurisdictional nature of cyberspace, as well as the sheer size of the challenge, requires closer collaboration with other federal, state, local, and international law enforcement partners.

Objective 4.1: Combat financial and trans-border cyber crimes and disrupt and defeat associated criminal organizations.

While our law enforcement jurisdiction is broad, DHS must continue to focus on our core investigative responsibilities regarding financial services and payment systems, computer fraud and abuse, cross-border transmission of illicit materials, human trafficking and child exploitation, intellectual property violations, misuse of cryptocurrencies, and other violations of customs law through the Internet or online marketplaces. DHS must prioritize investigative efforts to focus on identifying, disrupting, and dismantling transnational criminal organizations

[9] While multiple DHS Components have law enforcement responsibilities, those with the most direct responsibility related to countering illicit cyber activity include the United States Secret Service (USSS) and U.S. Immigration and Customs Enforcement Homeland Security Investigations (ICE/HSI).

and sophisticated criminals that constitute the most significant economic and homeland security threats to the Nation.

Sub-Objectives:

a. Develop DHS investigative priorities related to illicit cyber activity.
b. Identify and conduct high-impact investigations of cyber crimes and illicit uses of cyberspace by transnational criminal organizations.
c. Disrupt the ability to use online marketplaces and tools for illicit trafficking, money laundering, and malicious cyber activity.
d. Develop options to appropriately disrupt, counter, and deter transnational criminal organizations to augment arrest and prosecution of individual criminals.

Outcomes:

DHS law enforcement investigations effectively counter significant illicit cyber activities and the ability of transnational criminal organizations to operate online.

Objective 4.2: Prevent, disrupt, and counter cybersecurity threats to protected persons, special security events, and critical infrastructure.

DHS must fully leverage its law enforcement and protective capabilities to provide appropriate security for protected persons, special security events, federal facilities, and other high-risk critical infrastructure against cyber threats. DHS has been a leader in integrating traditional law enforcement methods and protective measures to strengthen security. Such efforts include working with national and international partners through electronic crimes task forces to prevent, detect, and investigate various cyber crimes, including potential terrorist attacks against critical infrastructure and financial payment systems, as well as improving the security of federal facilities. DHS must strengthen its ability to apply its full range of authorities in an integrated manner to counter cyber threats to protected persons, special security events, federal facilities, and other critical infrastructure.

Sub-Objectives:

a. Identify and investigate cyber threats to protected persons, special events, federal facilities, and other critical infrastructure.
b. Implement detection and protection measures to appropriately secure key systems and assets.

Outcomes:

DHS timely and thoroughly investigates key cyber threats to protected persons, events, and assets, and applies protective measures based on insight regarding such cyber threats.

Objective 4.3: Develop relationships and build law enforcement capacity to counter illicit uses of cyberspace.

Countering illicit uses of cyberspace requires enhanced law enforcement coordination and engagement. DHS must expand outreach to other law enforcement entities at the federal, state, local, territorial, and tribal levels. DHS must build on existing collaboration capabilities such as cyber crime centers and electronic crimes task forces, which join together law enforcement, the private sector, and academia for the purpose of preventing, detecting, and investigating various forms of cyber crimes. DHS must also expand our role in international cyber investigations and law enforcement working groups that target transnational criminal organizations through our numerous attachés located around the world, as well as with key international organizations such as Interpol and Europol. DHS must continue to provide training on cyber crime investigations and digital forensics to law enforcement partners, including equipping nonfederal agencies where appropriate.

Sub-Objectives:

a. Collaborate with other domestic law enforcement agencies to investigate and counter cyber crimes.
b. Strengthen partnerships with private industry and academia to prevent and counter illicit uses of cyberspace.
c. Strengthen international law enforcement partnerships to counter cyber crimes.
d. Provide training and, where appropriate, otherwise equip law enforcement partners to improve collective law enforcement capabilities.

Outcomes:

Greater cooperation with increasingly capable foreign and domestic law enforcement agencies results in apprehension of transnational criminal actors and dismantling of transnational criminal organizations that seek to use cyberspace for illicit purposes.

Objective 4.4: Develop capabilities and resources to enhance investigative efforts and address evolving law enforcement challenges.

DHS must better align our existing law enforcement efforts and resources to address new and emerging challenges in cyberspace, to include the growing use of end-to-end encryption, anonymous networks, online marketplaces, and cryptocurrencies. DHS must look for ways to leverage and share existing resources, technical capabilities, and investigative information available across the Department to counter illicit uses of cyberspace, and invest in new capabilities and development opportunities for law enforcement agents.

Sub-Objectives:

a. Identify and align existing DHS cyber investigative capabilities and mission support resources to build greater law enforcement capabilities.
b. Leverage technical capabilities and resources available across the Department to supplement and support existing investigative and forensic efforts.
c. Invest in cutting-edge technical resources and advanced law enforcement capabilities for DHS and its partners.

d. Develop a method for DHS to more effectively share our investigation-related information through a non-classified, law enforcement sensitive mechanism.

Outcomes:

DHS investigative and forensic capabilities and resources more effectively support investigations of sophisticated cyber criminals.

PILLAR IV – CONSEQUENCE MITIGATION

DHS must limit the impact of potentially significant cyber incidents by leveraging our unique emergency management expertise and insights from network protection and law enforcement efforts.

Goal 5:
Respond Effectively to Cyber Incidents

We will minimize consequences from potentially significant cyber incidents through coordinated community-wide response efforts.

As the world becomes ever-more connected, the number and scale of cyber incidents are certain to grow despite network protection and law enforcement best efforts. Many cyber incidents do not require a national response. But, where they do, DHS plays a unique role in responding to cyber incidents to mitigate potential consequences by providing technical assistance to affected entities and other assets that are at risk (asset response) and in investigating the underlying crimes (threat response).[10] DHS responds to significant cyber incidents in close coordination with the Department of Justice and other federal agencies. In our role as asset responder, DHS must enhance capabilities to protect entities from additional harm following an incident, reduce the risk to others, safeguard sensitive personal and business information, and coordinate responses to significant incidents. As part of the law enforcement community, DHS must investigate incidents and be prepared to identify and counteract immediate cyber threats.

DHS must also implement mechanisms to ensure that asset and threat responders, informed by the intelligence community, share information with each other, with sector specific agencies, and with the private sector to inform all related incident response efforts. DHS sector specific agencies must similarly be prepared to provide sector expertise to support the needs of federal responders, and to promote and support private sector coordination during and after a cyber incident. In the case of significant cyber incidents, DHS must ensure preparedness across our Components for a coordinated government-wide response and to support any related emergency management activities. DHS must also ensure that we have in place mechanisms to coordinate with international partners as cyber incidents, whether they originate domestically or abroad, assume international implications.

[10] Pursuant to Presidential Policy Directive 41, "United States Cyber Incident Coordination" (July 26, 2016).

Objective 5.1: Increase voluntary incident reporting and victim notification to facilitate the provision of response assistance.

DHS cybersecurity efforts must be directed to build trusted relationships with entities at greatest risk of experiencing potentially significant cyber incidents. These relationships, especially through DHS field offices and sector specific agencies, help to facilitate the provision of DHS and other federal resources following an incident. DHS must encourage the reporting of incidents, and work with other incident responders to develop consistent processes for notifying potential victims of cyber incidents. Encouraging a culture of reporting, notification, and information sharing will increase the security and resilience of critical infrastructure, help prevent, counter, and disrupt illicit cyber actors, and enable the government to assess and potentially manage responses to incidents of unknown severity.

Sub-Objectives:

a. Encourage reporting of cyber incidents by nonfederal entities to DHS or other law enforcement agencies, relevant sector specific agencies, and the National Cybersecurity and Communications Integration Center (NCCIC).
b. Improve processes to facilitate timely and effective notification to potential victims of cyber incidents by DHS and other agencies, and to enhance sector specific agency awareness of incidents within their sectors.

Outcomes:

DHS receives reports of cyber incidents and, in appropriate coordination with other agencies, makes timely victim notifications.

Objective 5.2: Expand asset response capabilities to mitigate and manage cyber incidents.

DHS provides asset response assistance to requesting entities following incidents that pose significant risks to national security, public health and safety, or economic security, or as otherwise appropriate to the circumstances. DHS is also responsible for maintaining shared situational awareness of emerging cybersecurity risks and incidents. During significant cyber incidents, DHS serves as the lead agency for asset response, as part of a Cyber Unified Coordination Group, and supports the White House-led Cyber Response Group. DHS must continue to build capabilities to provide technical assistance and mitigation recommendations, including on-site incident response teams, following cyber incidents. DHS must also leverage incident information to identify emerging risks and protect entities that rely on impacted entities or those at risk of similar incidents.

Sub-Objectives:

a. Develop technical asset response capabilities to respond to cyber incidents.
b. Establish a common operating picture across the Department and with other stakeholders to assess emerging incidents and associated national, regional, or sector risks.
c. Build capacity to manage national asset response efforts and support a Cyber Unified Coordination Group and Cyber Response Group following significant incidents.

d. Support emergency management efforts under the National Response Framework for cyber incidents that may result in physical impacts or otherwise impede disaster response and recovery efforts.
e. Plan and exercise for cyber incident response at the local, regional, national, and international level.

Outcomes:
DHS responds to cyber incidents by providing technical and other asset response assistance, where requested and appropriate, and supporting national-level decision-making and emergency management efforts.

Objective 5.3: Increase cooperation between incident responders to ensure complementary threat response and asset response efforts.

Threat response activities include efforts by DHS and non-DHS law enforcement agencies to combat cyber crimes and national security threats through investigations that identify malicious actors and seek to prevent or deter additional illicit cyber activity. Effective incident response requires an understanding of the methods and intent of the responsible threat actors as well as the provision of asset response assistance. DHS investigative and intelligence assets must collaborate with asset responders, other entities responding to incidents, and affected entities to share information regarding the threat to prevent additional harm. Such information must be integrated with information available from other law enforcement agencies, the intelligence community, and other sources. DHS must also promote effective coordination between all agencies responding to a cyber incident in the field to enhance the timeliness and effectiveness of response efforts.

Sub-Objectives:
a. Leverage DHS and non-DHS investigative resources to provide incident and threat attribution information to all federal incident responders and sector specific agencies.
b. Develop holistic assessments of adversaries, threats, and incidents to aid asset and threat response, as well as protective and planning efforts.
c. Improve mechanisms to increase field-level collaboration on cybersecurity issues and coordinate the provision of federal response assistance when appropriate.

Outcomes:
DHS responds to incidents and engages impacted entities in a coordinated fashion, enabling access to the expertise and capabilities of all threat and asset responders.

PILLAR V – ENABLE CYBERSECURITY OUTCOMES

DHS must enable improved cybersecurity risk management outcomes by supporting policy and operational efforts that make the entire cyber ecosystem more secure and reliable. These efforts help shift the advantage away from malicious cyber actors toward those protecting cyberspace. DHS must similarly look internally to align our efforts to maximize cybersecurity outcomes.

Goal 6: Strengthen the Security and Reliability of the Cyber Ecosystem

We will support policies and activities that enable improved global cybersecurity risk management.

A more fundamentally secure cyber ecosystem can help tip the balance toward those protecting networks and away from malicious cyber actors. Strengthening the security and reliability of the cyber ecosystem therefore enables risk management and sets the conditions to support other DHS strategic cybersecurity goals.

The cyber ecosystem includes not only the interconnected network of information technology infrastructure we call cyberspace, but also the people, environment, norms, and conditions that influence that network. DHS must support efforts globally that will result in fundamentally improved security outcomes through technological innovation as well as the widespread adoption of improved operational and policy frameworks. DHS must also invest in research and development efforts that support mission objectives. So, too, must DHS develop collaborative communities, build global partnerships, and participate in international and multi-stakeholder venues to advance positive developments in cybersecurity and to impose costs for unacceptable behavior in cyberspace. To create a pipeline to support our cybersecurity goals, DHS must accelerate the expansion of cyber personnel programs.

Objective 6.1: Foster improved cybersecurity in software, hardware, services, and technologies, and the building of more resilient networks.

DHS must support efforts to identify and develop high-leverage technical, operational, and policy innovations that will result in more secure technologies and resilient networks. Many of today's greatest challenges are endemic to the current ecosystem. Nearly all cyber incidents, for example, involve exploitation of vulnerabilities or misconfigurations in software or hardware. Network operators are also increasingly dependent on vendors of commercial off-the-shelf products or integrators of commercially available products, and lack the capability to effectively manage supply chain risks. The continued globalization of the information technology supply chain and shifting of information and services to cloud or other shared infrastructure introduces additional risks. As Internet-connected and other new technologies rapidly proliferate, the number of attack vectors also increases. Developers and manufacturers of many internet-of-

things and other consumer devices are frequently motivated by speed to market rather than strong security. Even specialized technologies, like medical devices and industrial control systems, remain susceptible to compromise.

DHS must foster innovations that can shift the status quo toward improved security and resilience. DHS must partner with information technology, communications, cybersecurity services, and other communities to incentivize security and enable cybersecurity outcomes such as minimizing vulnerabilities and addressing supply chain risks. DHS must also encourage improved security for cloud infrastructure and throughout the life-cycle of internet-of-things devices and emerging technologies. In addition, DHS must focus on efforts to enhance the overall resiliency of networks that can be vulnerable to a variety of attacks. DHS must leverage our unique expertise to support associated standards-setting efforts, and ensure all of our related activities are aligned with those of interagency and international partners to ensure consistency of approaches.

Sub-Objectives:

a. Identify and foster high-leverage innovations to drive more secure software, hardware, services, and technologies, and more resilient networks.
b. Develop solutions to identify and manage supply chain risks for federal networks and other national and global stakeholders.
c. Engage with relevant stakeholders to enhance cybersecurity of cloud infrastructure, internet-of-things products, and other emerging technologies or otherwise mitigate associated threats to networks.

Outcomes:

More secure and resilient technologies and networks result in a more defensible cyber ecosystem.

Objective 6.2: Prioritize DHS cybersecurity research, development, and technology transition activities to support DHS mission objectives.

DHS research and development efforts must continue to support and advance our cybersecurity objectives, including the development of protective capabilities to secure the federal enterprise and critical infrastructure and necessary tools for law enforcement. DHS must also prioritize research and development that supports incident response, information sharing, and other cybersecurity objectives identified in this strategy. DHS must leverage commercial capabilities and research and development efforts targeting information and communication technology. Where DHS invests in cybersecurity research and development, we must focus on capabilities and innovations that support departmental priorities and can be employed by DHS and other key stakeholders, to include private sector, state, local, tribal, territorial, and international partners.

Sub-Objectives:

a. Develop and implement effective methods to prioritize research and development needs based on identified DHS cybersecurity objectives.
b. Identify, develop, and transition new capabilities and innovations that support DHS cybersecurity objectives.

Outcomes:
New technologies resulting from Department-supported research and development increase the capability to protect critical systems, investigate cyber crimes, respond to cyber incidents, and accomplish identified DHS cybersecurity objectives.

Objective 6.3: Expand international collaboration to advance DHS objectives and promote an open, interoperable, secure, and reliable Internet.

DHS international cybersecurity engagements must help shape the cyber ecosystem to support the Department's cybersecurity objectives and broader U.S. foreign policy priorities. DHS develops and maintains relationships with international partners that advance our specific network protection, law enforcement, incident response, and research and development objectives. DHS also participates in international fora to support risk management objectives and broader cybersecurity goals, including the U.S. goal of an open, interoperable, secure, and reliable Internet. For example, DHS encourages widespread adoption of voluntary norms of responsible state behavior in peacetime to improve international stability and protect critical infrastructure. DHS also supports broader U.S. and international efforts to deter those who act unacceptably in cyberspace and impose costs on those actors. Developing the capacity of foreign Computer Security Incident Response Teams (CSIRTs) and law enforcement entities also enhances global cybersecurity efforts and supports broader DHS and U.S. foreign policy objectives.

Sub-Objectives:

a. Prioritize international engagements based on DHS and national objectives.
b. Improve international cooperation and build capacity through the sharing of best practices, cybersecurity information, expertise, and technical assistance.
c. Contribute cybersecurity subject matter expertise to advance efforts in international fora and advance positive international policy developments in cybersecurity.
d. Support efforts to impose costs for unacceptable behavior in cyberspace.

Outcomes:
DHS international engagements result in shared global approaches to cybersecurity and increased capabilities and cooperation on cybersecurity risk management activities.

Objective 6.4: Improve recruitment, education, training, and retention to develop a world-class cyber workforce.

There is a critical shortage of cybersecurity talent globally, as the demand for personnel with cyber expertise in both the public and private sectors far exceeds the supply. Execution of our cybersecurity responsibilities depends on the recruitment and retention of highly skilled cyber professionals, but career paths in cybersecurity are far more lucrative in the private sector and traditional federal hiring processes are not aligned to the culture of cyber recruitment and hiring. The challenge is not ours alone. Key stakeholders across government and in the private sector face similar shortfalls.

DHS must continue to support efforts to increase the supply of national cybersecurity talent through cyber education programs and the National Initiative for Cybersecurity Education (NICE). DHS must also continue to develop and promote cybersecurity training programs dedicated to advancing the cybersecurity skills of the existing federal workforce. DHS must, in particular, work to expand and accelerate our cybersecurity personnel recruitment, training, and retention efforts through congressionally mandated workforce analysis and planning actions and by implementing the authorized cybersecurity-focused personnel system with hiring and compensation flexibilities. DHS must also encourage and support the development and implementation of specifically designed training programs for our network protection and law enforcement personnel to support the needs of DHS and other stakeholders.

Sub-Objectives:

a. Assess participation in and continue support for cyber training, awareness, education, and retention initiatives to support the homeland security enterprise.
b. Complete mandatory DHS workforce planning and analysis activities to source data to drive approaches to recruitment, retention, and training.
c. Enhance cyber recruitment strategies across the Department to target highly skilled and trained populations to perform mission critical cyber activities.
d. Implement the full range of congressionally authorized cyber security human capital flexibilities for the Department.
e. Develop cutting-edge network protection and cyber investigative workforces through increased training, detail assignments, and advanced development opportunities.

Outcomes:

DHS recruits and trains highly-skilled cybersecurity personnel and develops a cadre of well-trained cybersecurity professionals across the Department and homeland security enterprise.

Goal 7:
Improve Management of DHS Cybersecurity Activities

We will execute our departmental cybersecurity efforts in an integrated and prioritized way.

Each of the cybersecurity goals identified in this strategy involves multiple Components. While some have major external responsibilities with respect to network protection or law enforcement, all are involved in protecting internal networks and program data, hiring cyber professionals, and acquiring secure information and communication technologies. To ensure departmental unity of effort and a coordinated approach to accomplishing our cybersecurity goals and objectives, DHS must constantly assess evolving risks and evaluate priorities in the cybersecurity mission space. DHS must also develop department-wide processes and policies to align Component programs and activities with this strategy, departmental priorities, and changes in the cybersecurity

landscape. Through these efforts, DHS must be positioned to address our evolving needs and to adapt to evolving cyber threats.

Objective 7.1: Integrate Department-wide cybersecurity policy development, strategy, and planning activities.

Through PLCY, and in collaboration with the DHS Management Directorate and affected Components, we must establish internal mechanisms to ensure the development and execution of consistent cybersecurity policy and strategic plans. DHS must effectively collaborate across Components to promote and ensure consistent and integrated programs and activities.

Sub-Objectives:

a. Identify and expand internal coordination mechanisms to ensure consistent departmental approaches to cybersecurity policy development and strategy and to accomplish identified cybersecurity goals and objectives.
b. Establish mechanisms to integrate and align cross-Component cyber activities.

Outcomes:

DHS will execute our cybersecurity mission responsibilities in a coordinated and integrated way.

Objective 7.2: Prioritize and evaluate the effectiveness of DHS cybersecurity programs and activities.

DHS must ensure that our cybersecurity programs and activities align to the goals and objectives set forth in this strategy. DHS must leverage management processes to evaluate programs and activities to assess their efficacy and to ensure that program funding, personnel, and other resources are optimized to meet departmental priorities.

Sub-Objectives:

a. Prioritize cyber related programming and activities across the Department in accordance with this strategy.
b. Review and evaluate the effectiveness of DHS cyber programs and activities and alignment to budget, programmatic, and policy efforts.
c. Identify and prioritize gaps, through the Department's joint requirements process, across all the goals and objectives of this strategy.

Outcomes:

DHS cybersecurity programs effectively and efficiently address departmental goals and objectives.

CONCLUSION

DHS believes that cyberspace can be made safe and secure for the functioning of government, the delivery of essential services, and the everyday lives of the American people. DHS will maintain a leadership role, collaborating with other federal agencies, the private sector, and other stakeholders, across all of its cybersecurity mission areas to ensure that cybersecurity risks are effectively managed, critical networks are protected, vulnerabilities are mitigated, cyber threats are reduced and countered, incidents are responded to in a timely way, and the cyber ecosystem is more secure and resilient. Meeting the goals and objectives outlined in this strategy requires a unified, long-term approach across the Department. Aligning departmental network protection and law enforcement authorities with traditional risk management, information sharing, and incident response efforts will enhance DHS cybersecurity efforts moving forward and provide the Nation with a secure cyberspace for future generations.

APPENDIX: DHS CYBERSECURITY AUTHORITIES

Statutes

- **Title II of the Homeland Security Act of 2002, as amended (Pub. Law 107-296):** Subtitle B of title II authorizes DHS, through NPPD, to enhance the security, resilience, and reliability of the Nation's cyber and communications infrastructure—

  Section 227 – National cybersecurity and communications integration center (6 U.S.C. § 148). Created by the National Cybersecurity Protection Act of 2014 (Pub. Law 113-282) and amended by the Cybersecurity Act of 2015, section 227 authorizes the NCCIC within NPPD as a "Federal civilian interface for the multi-directional and cross-sector sharing of information related to … cybersecurity risks." This provision includes the authority to receive, analyze, and disseminate information about cybersecurity risks and incidents and to provide guidance, assessments, incident response support, and other technical assistance upon request. Section 227 codifies NPPD's coordinating role among federal and nonfederal entities, and clarifies that NPPD's cybersecurity authorities apply broadly to federal and nonfederal entities, including international partners, sectors of critical infrastructure, information sharing organizations, or any other entity. Section 227 also authorizes NPPD to establish information sharing relationships, and to enter into information sharing agreements, and establishes a wide range of federal and nonfederal stakeholders as components of the NCCIC.

  Section 223 – Enhancement of Federal and Non-Federal Cybersecurity (6 U.S.C. § 143). Section 223 authorizes NPPD, in carrying out its cybersecurity responsibilities, to provide "analysis and warnings related to threats to, and vulnerabilities of, critical information systems" to state and local government entities, and upon request to owners and operators of critical information systems. Section 223 also authorizes NPPD to provide "crisis management support" and "technical assistance," including recovery assistance, to the private sector and governmental entities. Section 223 also delegates to NPPD the Department's responsibilities to protect federal information systems under subchapter II of chapter 35 of title 44 (discussed below).

  Section 201(d) (6 U.S.C. § 121(d)). Section 201 broadly authorizes NPPD's activities to ensure security and resilience of critical infrastructure to terrorist and other threats, including by authorizing NPPD to access and integrate information, as well as to carry out comprehensive assessments of the vulnerabilities of critical infrastructure.

  Section 228 – Cybersecurity plans (6 U.S.C. § 149). Section 228, as amended by the Cybersecurity Act of 2015, directs DHS to develop, maintain, update, and exercise cyber incident response plans – including "the National Cybersecurity Incident Response Plan and the Cyber Incident Annex to the National Response Framework." The NCCIC is specifically required to participate in national exercises associated with those plans.

Section 230 – Federal intrusion detection and prevention system (6 U.S.C. § 151 & 151 note). The Federal Cybersecurity Enhancement Act of 2015 created section 230 of the Homeland Security Act, which authorizes DHS to deploy technology that detects and removes cybersecurity risks in information transiting or traveling to and from agency systems, notwithstanding any other provision of law. The Act mandates that all agencies "apply and continue to utilize" DHS technologies authorized by this section, including improvements and new capabilities that DHS makes available within six months.

Section 226 – Cybersecurity recruitment and retention (6 U.S.C. § 147). The Border Patrol Agent Pay Reform Act of 2014 (Pub. Law 113-277) amended the Homeland Security Act to authorize the Secretary to establish cybersecurity positions, appoint personnel, fix rates of pay and promulgate implementing regulations in consultation with the director of the Office of Personnel Management (OPM).

- **The Cybersecurity Information Sharing Act of 2015 (CISA) (Title I of the Cybersecurity Act of 2015)** (6 U.S.C. §§ 1501-1510). CISA requires DHS, in consultation with interagency partners, to establish the Federal Government's capability and process for receiving cyber threat indicators and defensive measures, and directs DHS to further share cyber threat indicators and defensive measures it receives with federal entities in an automated and real-time manner. CISA provides targeted liability protection to companies that share cyber threat indicators with DHS and provides other legal protections for indicators shared in accordance with CISA. CISA also authorizes private entities to share cyber threat indicators with one another and to monitor their networks for cybersecurity threats, with liability protection for doing so, as well as to operate defensive measures.

- **Subchapter II of Chapter 35 of Title 44** (44 U.S.C. §§ 3551-3558). These provisions, created by the Federal Information Security Modernization Act of 2014 (Pub. Law 113-283), direct the Secretary to provide information protections for DHS networks commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of DHS information or information systems. The provisions also establish DHS's central role in the security of the information and information systems of federal executive branch agencies. Through NPPD, DHS administers the implementation of government-wide policies, deploys technologies to assist in the protection of federal agencies' networks information and information systems, and issues binding operational directives to agencies to safeguard information and information systems. The Act also places in DHS the federal information security incident center.

- **Strengthening State and Local Cyber Crime Fighting Act of 2017, Pub. Law 115-76,** (6 U.S.C. § 383**)**. The Act amended the Homeland Security Act, adding a section 822, to authorize the USSS to operate the National Computer Forensics Institute to disseminate information related to the investigation and prevention of cyber and electronic crime and related threats, and educate, train, and equip state, local, tribal, and territorial law enforcement officers, prosecutors, and judges, and facilitate the expansion of the network of Electronic Crime Task Forces of the USSS.

- **Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, as amended** (18 U.S.C. §§ 1029-1030). The Act amended the federal criminal code to establish an offense of fraud in connection with computers and grants authority to the USSS to investigate offenses under this Act. As amended, the Act establishes criminal violations related to cybersecurity, such as obtaining information or causing damage by intentionally accessing, without authorization, a computer which is used in or affecting interstate or foreign commerce or communication.

- **18 U.S.C. § 3056**. Authorizes the USSS to assess and mitigate cybersecurity risks to systems that could impact the agency's protective mission, as well as detect and arrest any person who violates the laws of the United States relating to electronic fund transfer frauds, access device frauds, false identification documents or devices, and any fraud or other criminal or unlawful activity in or against any federally insured financial institution, among other violations.

- **18 U.S.C. § 3056 note (Expansion of National Electronic Crime Task Force Initiative)**. Requires the USSS "to develop a national network of electronic crime task forces, based on the New York Electronic Crimes Task Force model, throughout the United States, for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems."

- **Section 890A of Title VIII of the Homeland Security Act** (6 U.S.C. § 473). The Human Exploitation Rescue Operations (HERO) Act of 2015 (Pub. Law 114-22) amends title VIII of the Homeland Security Act and directs the Department to operate, within HSI, a Cyber Crimes Center to provide investigative assistance, training, and equipment to support domestic and international investigations by HSI of cyber-related crimes. The HERO Act also creates a Cyber Crimes Unit (CCU) within the Cyber Crimes Center, which oversees the cyber security strategy and cyber-related operations and programs for HSI.

- **18 U.S.C. § 1028A – Aggravated Identify Theft**. The USSS and other federal law enforcement agencies investigate violations of the prohibition against an individual who "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable State or local law."

- **18 U.S.C. §§ 2251, 2252, 2260 – Sexual exploitation of children, child pornography, importation of sexually explicit depictions of a minor**. These subsections of Title 18 criminalize the sexual exploitation, activities, and importation of material involving and constituting the exploitation and distribution of child pornography. HSI has primary investigative jurisdiction of child pornography involving international transportations, shipping, and mailings.

- **18 U.S.C. § 2319 and 17 U.S.C. § 506 – Criminal Infringement of a copyright**. HSI investigates violations of these subsections which criminalize the willful act of infringing a copyright.

- **Federal Cybersecurity Workforce Assessment Act - part of the Consolidated Appropriations Act of 2016, P.L. 114-113 (Dec 18, 2015).** The Federal Cybersecurity Workforce Assessment Act of 2015 was enacted in December 2015. It assigned specific workforce planning-related activities to all federal agencies, including DHS. Specifically, the law requires all federal agencies to identify all positions that perform information technology, cybersecurity, or other cyber-related functions and assign the appropriate employment code to each position. The Act also requires all federal agencies, including DHS, to identify and report to OPM on its cybersecurity work roles of critical need; each agency also is to submit a progress report on identifying cyber-related work roles of critical need to Congress.

- **Border Patrol Agent Pay Reform Act, P.L. 113-277 (Dec 18, 2014)** (6 U.S.C. § 146)**.** Section 3 of this Act directs the Secretary of Homeland Security, within 180 days and annually thereafter for three years, to conduct an assessment of the DHS cybersecurity workforce. The Act also directs the Secretary to develop, maintain, and update a comprehensive workforce strategy to enhance the readiness, capacity, training, recruitment, and retention of DHS's cybersecurity workforce. Section 4 of this Act requires the Secretary to submit to the appropriate congressional committees: (1) annual updates on such assessment and on the Secretary's progress in carrying out such strategy; and (2) a report on the feasibility, cost, and benefits of establishing a Cybersecurity Fellowship Program to offer a tuition payment plan for individuals pursuing undergraduate and doctoral degrees who agree to work for DHS for an agreed upon period.

- **Cybersecurity Workforce Assessment Act, P.L. 113-246 (Dec. 18, 2014)** (6 U.S.C. § 146 note)**.** Authorizes the Secretary to identify, determine, and assign the appropriate employment codes, work categories, and specialty areas of critical need to enable the Secretary to effectively implement the Cybersecurity Workforce Assessment Act.

- **49 U.S.C. § 44912 (b)(1)(A)(ii)(b) 'REVIEW OF THREATS.'** This section directs the TSA to periodically review threats to civil aviation, with particular focus on a comprehensive systems analysis of the civil aviation system, including: (i) the destruction, commandeering, or diversion of civil aircraft or the use of civil aircraft as a weapon; and (ii) the disruption of civil aviation service, including by cyberattack.

- **46 U.S.C. § 3306**. Addresses USCG Officer in Charge, Marine Inspection (OCMI) authorities over vessel safety. As the Maritime Transportation sector specific agency, these authorities support USCG regulatory oversight of commercial vessels, to include cyber security equities associated with safety management systems.

- **46 U.S.C. § VII**. Addresses OCMI and Captain of the Port (COTP) authorities over vessel and facility security. It also designates USCG officials as Federal Maritime Security Coordinators for areas in which Area Maritime Security Plans apply. From a cybersecurity

perspective, these authorities support the USCG's role as the Maritime Transportation sector specific agency.

- **Maritime Transportation Security Act of 2002, Public Law 107-85** (46 U.S.C. § 701). The Act provides authority for USCG to introduce cybersecurity requirements for both vessels and facilities through Facility Security Plans and Vessel Security Plans.

Executive Orders

- **Executive Order 13800—Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (2017)**. Directs federal agencies to conduct risk reviews and prepare reports related to the cybersecurity of federal networks, critical infrastructure, international cooperation and deterrence, and workforce development.

- **Executive Order 13773—Enforcing Federal Law with Respect to Transnational Criminal Organizations and Preventing International Trafficking (2017)**. Sets U.S. policy to strengthen enforcement of federal law in order to thwart transnational criminal organizations, to include those engaged in activity related to corruption, cyber crime, fraud, financial crimes, and intellectual property theft. The Secretary of Homeland Security is directed to work with the Attorney General, Secretary of State, and Director of National Intelligence, to implement the executive order.

- **Executive Order 13691—Promoting Private Sector Cybersecurity Information Sharing (2015)**. Tasks DHS with encouraging the development and formation of Information Sharing and Analysis Organizations (ISAOs) and entering into an agreement with a nongovernmental organization to serve as the ISAO Standards Organization to identify a common set of voluntary standards or guidelines for the creation and functioning of ISAOs under the executive order.

- **Executive Order 13636—Improving Critical Infrastructure Cybersecurity (2013)**. Directs the Department to increase its cybersecurity information sharing efforts with the private sector, consult on and promote the National Institute of Standards and Technology Cybersecurity Framework, and identify, develop, and maintain a list of critical infrastructure entities where a cybersecurity incident could reasonably result in catastrophic effects on the Nation.

Other Presidential Direction

- **Presidential Policy Directive 41—Cyber Incident Coordination Policy (2016)**. Sets forth principles governing the Federal Government's response to any cyber incident and, for significant cyber incidents, establishes an architecture for coordinating the broader response and recovery efforts, through a Cyber Unified Coordination Group with lead federal agencies responsible for coordinating respective lines of effort. During a significant incident, DHS, acting through the NCCIC, is the federal lead agency for asset response activities. DHS also takes information from a given incident and shares it more broadly, so that others will be protected against the same or similar threats. During a significant incident, the Department

of Justice, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, is the federal lead agency for threat response activities. USSS and ICE/HSI are responsible for investigating cyber crimes within their jurisdiction and, in the context of a significant cyber incident, will coordinate their threat response activities with the Department of Justice.

- **Presidential Policy Directive 21—Critical Infrastructure Security and Resilience (2013)**. Directs the Department to develop and implement strategic approaches to increase situational awareness of physical and cyber threats to infrastructure, and reinforces the need for holistic thinking about security and risk management.

- **Presidential Policy Directive 8 – National Preparedness (2011)**. Directs the Department to lead and coordinate the development of the national preparedness system, which includes "a series of integrated national planning frameworks." The National Response Framework is part of this national preparedness system and "sets the strategy and doctrine for how the whole community builds, sustains, and delivers the Response core capabilities identified in the National Preparedness Goal in an integrated manner with the other mission areas."

- **National Security Presidential Directive-54/Homeland Security Presidential Directive-23—Cybersecurity Policy (2008)**. Sets forth aspects of the Department's operational role, particularly in protecting federal information systems.

- **Homeland Security Presidential Directive 5 - Management of Domestic Incidents, as amended (2003)**. Enhances the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system (NIMS). This directive designates the Secretary of Homeland Security as the principal federal official for domestic incident management and provides that the Secretary shall coordinate the Federal Government's resources utilized in response to or recovery from terrorist attacks, major disasters, or other emergencies if and when any one of four specific conditions applies, including where one or more federal department or agency is substantially involved in the incident response.