

UNITED STATES COAST GUARD

★ ★ ★ ★

CYBER STRATEGY

JUNE 2015
WASHINGTON, D.C.

THE U.S. COAST GUARD'S VISION
FOR OPERATING
IN THE CYBER DOMAIN

*We will ensure the security of our cyberspace,
maintain superiority over our adversaries,
and safeguard our Nation's
critical maritime infrastructure.*

Table of Contents

I. Introduction	9
II. Executive Summary	11
III. Today's Realities	13
IV. U.S. Coast Guard and Cyber Operations	19
V. Strategic Priority: Defending Cyberspace	23
VI. Strategic Priority: Enabling Operations	27
VII. Strategic Priority: Protecting Infrastructure	31
VIII. Ensuring Long-Term Success	35
IX. Conclusion	39
X. Appendix	41



THE COMMANDANT OF THE UNITED STATES COAST GUARD



For more than two centuries, the U.S. Coast Guard has performed increasingly complex missions in the most challenging of marine environments. Throughout this history, the Coast Guard has continually adapted to the emergence of innovative technologies while leveraging new capabilities to ensure the safety, security, and stewardship of our Nation's waters. Today's rapidly evolving cyber domain presents unprecedented challenges and opportunities for our Service, as we help ensure our Nation's security and prosperity in this new century.

Cyber technology is inextricably linked with all aspects of Coast Guard mission performance. It simultaneously presents opportunities for greater efficiency and effectiveness in our operating environment, while fueling new threats and challenges. The Nation's security and prosperity is critically reliant on a safe and secure maritime domain, where threats and risks to our Nation and oceans are effectively managed and maritime commerce continues to thrive. To ensure the Coast Guard meets our Nation's most enduring maritime priorities, we must always ensure we meet our strategic priorities in the cyber domain.

I am pleased to introduce the U.S. Coast Guard's Cyber Strategy to guide our efforts in the cyber domain. This strategy identifies three distinct strategic priorities that are critical to our overall mission success: **Defending Cyberspace, Enabling Operations, and Protecting Infrastructure**. It also details a number of cross-cutting enabling factors that will ensure our long-term success.

The Coast Guard must adapt to the ongoing and rapid advancements in cyber technology. In continuing our proud history of responding to the ever evolving maritime needs of the Nation, the Coast Guard will fully embrace cyberspace as an operating domain. To this end, we will work tirelessly to achieve our vision for operating in the cyber domain: *"We will ensure the security of our cyberspace, maintain superiority over our adversaries, and safeguard our Nation's critical maritime infrastructure."*

Semper Paratus.

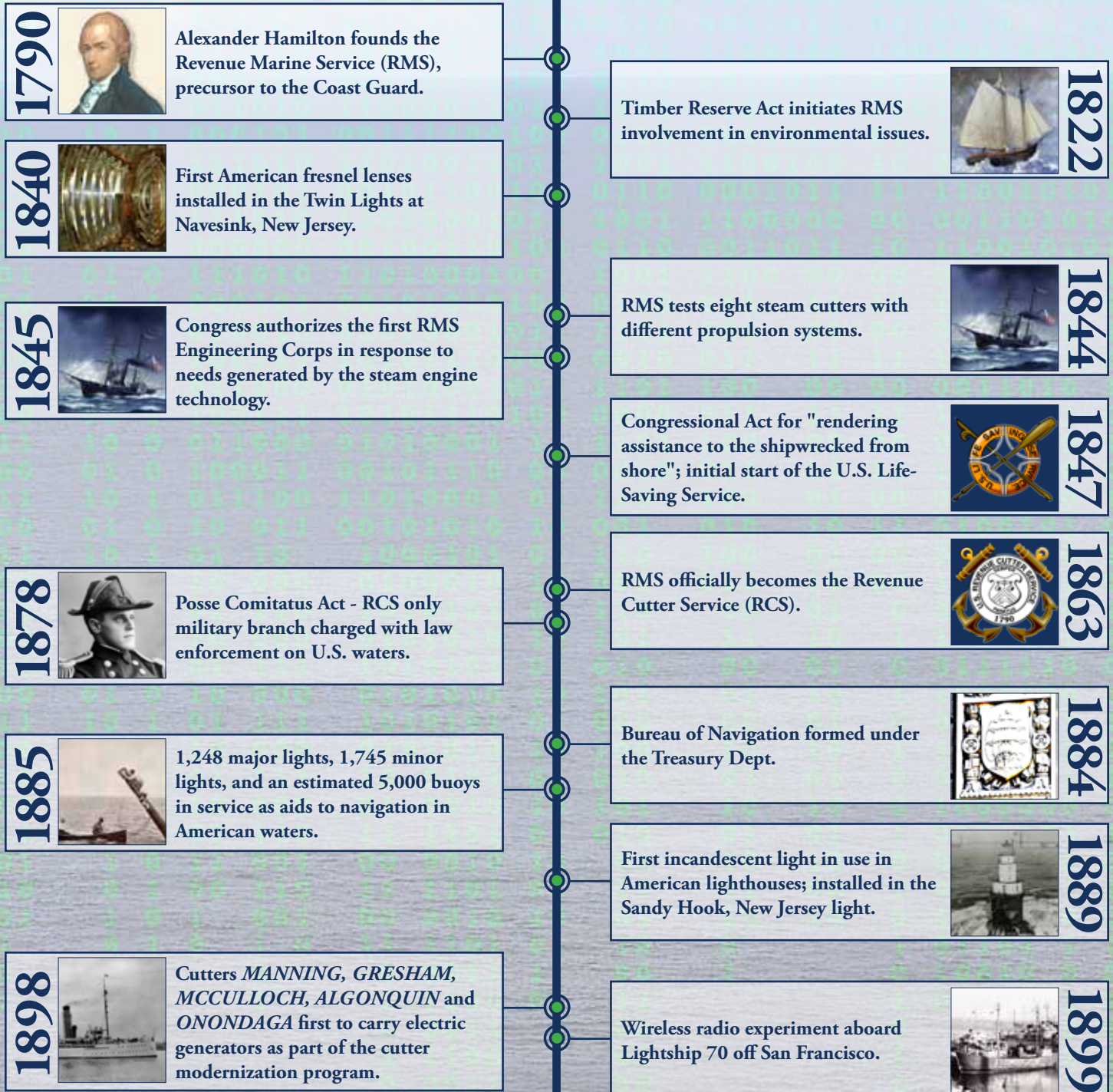
A handwritten signature in blue ink, reading "Paul F. Zukunft".

Admiral Paul F. Zukunft
Commandant

A BRIEF COAST GUARD HISTORY

Evolving with Technology & Mission

The Coast Guard has a long and rich history of adjusting to the ever evolving maritime needs of the Nation as well as the introduction of new technologies in the maritime domain. Below is a brief history of some of the mission challenges the Coast Guard (which includes Coast Guard precursor organizations such as the Revenue Marine Service, the Revenue Cutter Service, Lifesaving Service, etc.) has adapted to over time, as well as the technologies that have driven rapid change in the Coast Guard's operating environment.



1904



GRANT is first cutter to use radio for tactical purposes.

1915



Woodrow Wilson combines the Life-Saving Service and Steamboat Inspection with the RCS to found the modern U. S. Coast Guard.

1920



The first use of portable HF/DF leading to the interception and decryption of over 10,000 encrypted Rum Runner codes.

1942



Coast Guard Unit 387 was the first in the US to crack 3 kinds of enigma codes during WWII.

1944



The Office of Strategic Services, precursor to the CIA, and the Coast Guard create joint maritime units.

1958



Atlantic Merchant Vessel Emergency Reporting (AMVER) System relays ship's position info; invaluable to search and rescue missions.

1970



Water Quality Act increases Coast Guard jurisdiction over hazardous spills.

1991



Joint Maritime Information Element established at Operations Systems Center Martinsburg, W. Va.

2003



Coast Guard transferred from the Dept. of Transportation to the Dept. of Homeland Security.

Motorboat Act increases RCS responsibility to monitor boating safety requirements.



1910

Coast Guard Communication Division founded; 3671 miles of cable connects 282 stations, 44 units, and 139 lighthouses.



1919

The first Coast Guard cutter equipped with SIGINT for the purpose of interception and interdiction of Rum Runners during Prohibition.



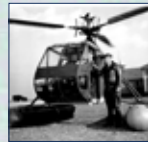
1929

American development of Long Range Aids to Navigation (LORAN); allows ships and planes to pinpoint their positions with accuracy.



1942

First use of a Coast Guard helicopter in a rescue mission.



1944

Transfer to Dept. of Transportation increases Coast Guard responsibility for economic traffic, migrant interdiction, and hazardous cargo.



1967

Oil Fingerprinting developed by the Coast Guard Research and Development Center (RDC).



1975

RDC develops the Differential Global Positioning System (DGPS).



1987

RDC develops the Automated Information System (AIS) to track ships.



1998

CG Cyber Command is established.



2013





I.

Introduction

Cyber technology* has changed our world. The ongoing digital revolution has fueled unprecedented prosperity and efficiency in our globalized economy, and has become inextricably linked with all aspects of our modern life. These innovations will continue to drive global progress for the foreseeable future, and by most accounts will continue to evolve at astonishing speeds. In the wake of this progress lie a growing number of challenges and risks that threaten the very core of our Nation's security and prosperity.

Cybersecurity* is one of the most serious economic and national security challenges we face as a Nation. Government systems—including Coast Guard systems—face a mounting array of emerging cyber threats that could severely compromise and limit our Service's ability to perform our essential missions. Our adversaries employ sophisticated tools and possess substantial resources. They include state-sponsored and independent hacker groups, terrorists, Transnational Organized Crime groups, as well as corrupt, disgruntled, and complacent employees (commonly referred to as insider threats). These growing threats also pose significant risks to our Nation's Maritime Transportation System (MTS) and critical infrastructure,* and by direct extension, our Nation's security and economic stability. With approximately 360 sea and river ports, which handle more than \$1.3 trillion in annual cargo, our Nation is critically dependent on a safe, secure, and efficient MTS, which in-turn is highly dependent on a complex, globally-networked system of automated cyber technology.

To meet the vast array of challenges in the digital age, the Coast Guard must strategically adapt. First and foremost, the Coast Guard must fully embrace cyberspace as an operational domain. To operate effectively within the cyber domain,* and to counter and protect against maritime cyber threats over the next decade, the Coast Guard's Cyber Strategy emphasizes three strategic priorities:

- **Defending Cyberspace**
- **Enabling Operations**
- **Protecting Infrastructure**

In addition to the three strategic priorities, this Strategy presents a framework of cross-cutting support factors that will ensure the Coast Guard's long-term success. These enabling concepts will be critical to meeting each of our strategic priorities.

* Denotes first use of term in this strategy; term defined in Appendix 1.



The overall mission of the U.S. Coast Guard is to ensure the Safety, Security, and Stewardship of our Nation's waters. In the digital age, however, there is no strategic objective the Coast Guard can adequately meet—or operational mission the Coast Guard can fully perform—without a robust and comprehensive cyber program.* This Strategy provides a framework for the Coast Guard's efforts in the cyber domain over the next ten years, which will be essential to ensuring our Nation's security and prosperity in the maritime environment. This framework will enable success across all Coast Guard mission areas, and will support all aspects of our "Prevent-Respond" core operational concept. It is aligned with current governing executive directives, policies, and laws, including (but not limited to) the *Maritime Transportation Security Act*, *Executive Order 13636*, *Presidential Policy Directive 21*, the *Department of Homeland Security Blueprint for a Secure Cyber Future* (2011), the *2014 DHS Quadrennial Homeland Security Review*, the *National Infrastructure Protection Plan of 2013*, and the *Department of Defense Cyber Strategy of 2015*.

The U.S. Coast Guard's Vision for Operating in the Cyber Domain:

We will ensure the security of our cyberspace, maintain superiority over our adversaries, and safeguard our Nation's critical maritime infrastructure.*



II.

Executive Summary

The Coast Guard is committed to ensuring the safety, security, and stewardship of our Nation's waters. This commitment requires a comprehensive cyber strategy that provides a clear framework for our overall mission success.

Cyber technology has fueled great progress and efficiency in our modern world. Coast Guard operations are more effective because of the rapid evolution in cyber technology, and advanced technologies have also led to an unprecedented era of efficiency of the Maritime Transportation System (MTS). However, with these benefits come serious risks. Information and its supporting systems are continually attacked and exploited by hostile actors. Foreign governments, criminal organizations, and other illicit actors attempt to infiltrate critical government and private sector information systems, representing one of the most serious threats we face as a nation.

As the Coast Guard relies on modern digital information and communications systems to execute its missions, the Service must defend against those who threaten them. The Coast Guard must also build and sustain an operational advantage in cyberspace to ensure optimal integration of information and intelligence with our operations. Moreover, the Coast Guard must lead the effort to protect maritime critical infrastructure from a broadening array of cyber threats.

To fully ensure the Coast Guard is able to perform its essential missions in the 21st Century, it must fully embrace cyberspace as an *operational domain*. To this end, the Coast Guard will focus on three specific strategic priorities in the cyber domain over the next ten years:

- **Defending Cyberspace**
- **Enabling Operations**
- **Protecting Infrastructure**

Defending Cyberspace: Secure and resilient Coast Guard IT systems and networks are essential for overall mission success. To ensure the full scope of Coast Guard capabilities are as effective and efficient as possible, the Coast Guard must serve as a model agency in protecting information infrastructure and building a more resilient Coast Guard network.

Enabling Operations: To operate effectively within the cyber domain, the Coast Guard must develop and leverage a diverse set of cyber capabilities and authorities. Cyberspace operations,* inside and outside Coast Guard information and communications networks and systems, can help detect, deter, disable, and defeat adversaries. Robust intelligence, law enforcement, and maritime and military cyber programs are essential to enhancing the effectiveness of Coast Guard operations, and deterring, preventing, and responding to malicious activity targeting critical maritime infrastructure. Coast Guard leaders must recognize that cyber capabilities are a critical enabler of success across all missions, and ensure that these capabilities are leveraged by commanders and decision-makers at all levels.

Protecting Infrastructure: Maritime critical infrastructure and the MTS are vital to our economy, national security, and national defense. The MTS includes ocean carriers, coastwise shipping along our shores, the Western Rivers and Great Lakes, and the Nation's ports and terminals. Cyber systems enable the MTS to operate with unprecedented speed and efficiency. Those same cyber systems also create potential vulnerabilities. As the maritime transportation Sector Specific Agency (as defined by the National Infrastructure Protection Plan), the Coast Guard must lead the unity of effort required to protect maritime critical infrastructure from attacks, accidents, and disasters.

Ensuring Long-term Success: In support of the three strategic priorities, this Strategy identifies a number of cross-cutting support factors that will ensure the Coast Guard's long-term success in meeting the Service's strategic goals in the cyber domain. These include:

- (1) recognition of cyberspace as an operational domain,***
- (2) developing cyber guidance and defining mission space,***
- (3) leveraging partnerships to build knowledge, resource capacity, and an understanding of MTS cyber vulnerabilities,***
- (4) sharing of real-time information,***
- (5) organizing for success,***
- (6) building a well-trained cyber workforce, and***
- (7) making thoughtful future cyber investments.***



III.

Today's Realities

The global information infrastructure, including telecommunications, computer networks, and their data, is critical to most aspects of modern life. Digital information systems and networks facilitate the timely, efficient, and effective operation of the critical services that our society depends upon, including those provided by both public and private sectors.

This section provides background information regarding a number of trends and realities that will inform the Coast Guard's strategic approach in addressing the future threats and challenges in the cyber domain.

A Double-Edged Domain

Industry will continue to drive the rapid acceleration of technological advancements in cyberspace. Consumer demand in both private and public sectors funds perpetual cycles of innovation that drive productivity and efficiency. These innovations have led to an interconnected and more productive world, but have also created new vulnerabilities and risks for virtually all consumers, businesses, organizations, and governments.

Cyber Threats – Types, Tools, and Trades

Emerging cyber threats are diverse and complex. Threats consist of a variety of state and non-state actors, Transnational Organized Crime (TOC) groups, so-called “hacktivists,” as well as terrorists. The tools these adversaries employ are as diverse as their motives and capabilities. A detailed breakdown of the most common cyber incidents on government systems can be found on the bottom of page 15.

Government Systems as Targets

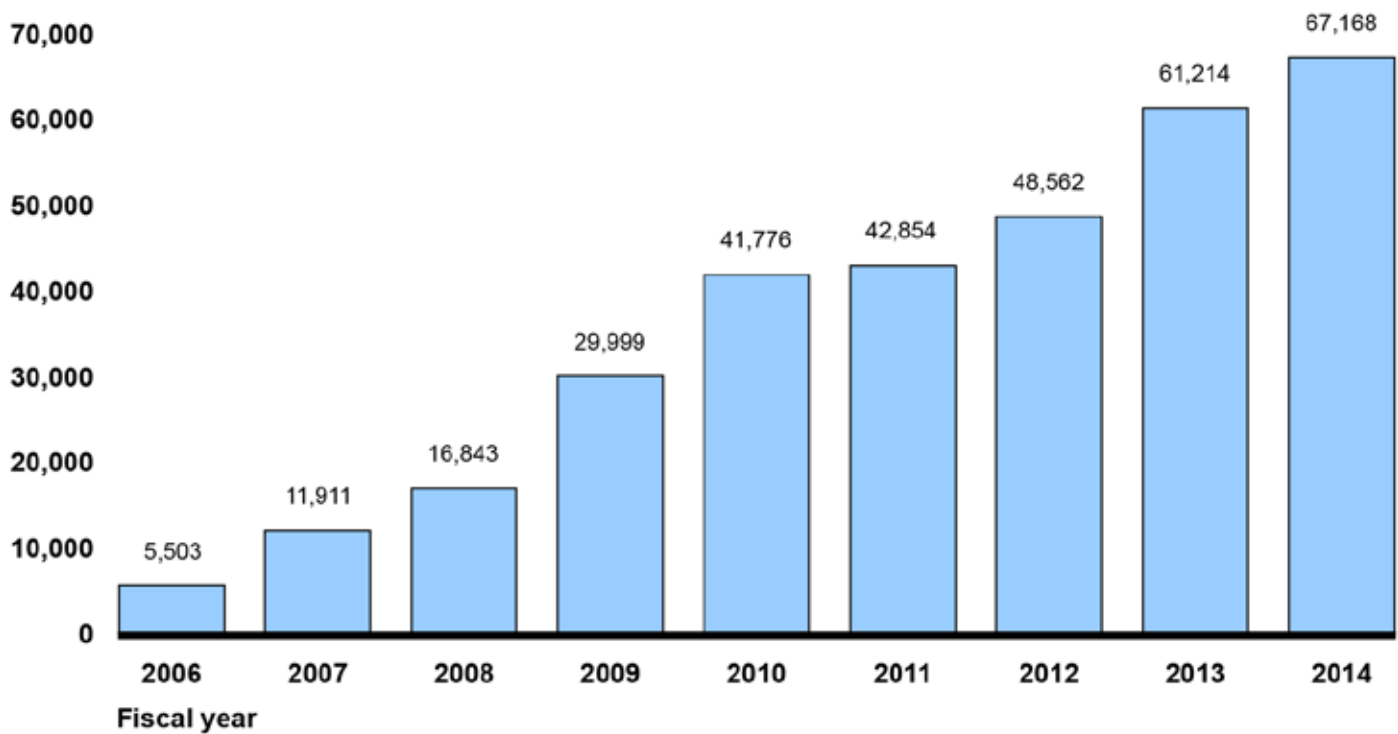
Classified and unclassified U.S. Government systems are constant targets of cyber attacks. Foreign intelligence* and security services, as well as non-state actors, actively target government networks to meet their strategic objectives. Many of these actors have penetrated government systems, causing potentially profound impacts to our national security.¹

In 2015, the Government Accountability Office (GAO) noted a 1,121 percent rise in cybersecurity incidents reported by government agencies from 2006 to 2014. The report also cites a significant rise in the compromise of sensitive information, which could “adversely affect national security; damage public health and safety; and lead to inappropriate access to and disclosure, modification, or destruction of sensitive information.” It also indicates disturbing

¹ Clapper, J (March 12, 2013). Worldwide Threat Assessment of the U.S. Intelligence Community, Statement for the Record. Senate Select Committee on Intelligence. Retrieved from: <http://www.intelligence.senate.gov/130312/clapper.pdf>.

INCREASING CYBER INCIDENTS:

Cyber Incidents Reported by Government Agencies



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-573T

trends in the availability and use of hacking tools, as well as advancements in the sophistication and effectiveness of attack technology.²

Risks to Critical Infrastructure

Adversaries are increasingly turning their attention to cyber vulnerabilities in our Nation's critical infrastructure.³ The Nation's increasing reliance on the essential goods and services these infrastructures provide exacerbates the ultimate impact cyber attacks could have on the economy.

As stated in Presidential Policy Directive 21 on Critical Infrastructure Security and Resilience, our Nation's critical infrastructure is diverse and complex. "It consists of distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations."⁴

The Department of Homeland Security (DHS) oversees the protection and resiliency of our Nation's critical infrastructure. DHS issued updated guidance for the national effort to manage risk to Critical Infrastructure Sectors in 2013 through the National Infrastructure Protection Plan. This National Plan identified the following goals in protecting national critical infrastructure from both physical and cyber threats:

² Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems, *GAO Testimony Before the Committee on Oversight and Government Reform, House of Representatives: GAO-15-573T*, pg. 6-8, April 22, 2015. Retrieved from: <http://www.gao.gov/assets/670/669810.pdf>.

³ Clapper, J (March 12, 2013). Worldwide Threat Assessment of the U.S. Intelligence Community, Statement for the Record. *Senate Select Committee on Intelligence*. Retrieved from: <http://www.intelligence.senate.gov/130312/clapper.pdf>.

⁴ *Presidential Policy Directive—Critical Infrastructure Security and Resilience*, Presidential Policy Directive/PPD 21, February 12, 2013. Retrieved from: <https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

- Identify, deter, detect, disrupt, and prepare for threats and hazards to the Nation's critical infrastructure;
- Reduce vulnerabilities of critical assets, systems, and networks; and
- Mitigate the potential consequences to critical infrastructure of incidents or adverse events that do occur.

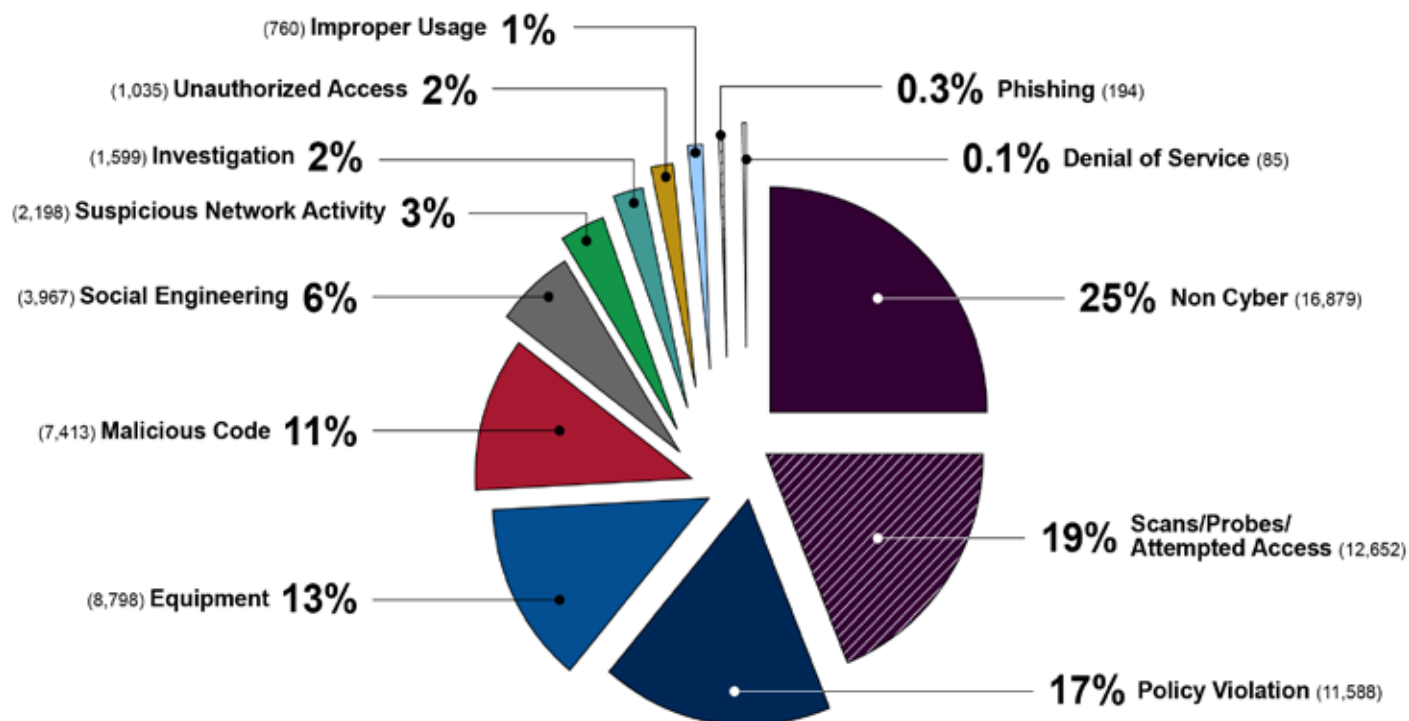
Maritime Critical Infrastructure and the Maritime Transportation System (MTS)

The Nation's security and prosperity depends upon a safe, secure, and resilient maritime critical infrastructure. America's MTS moves people, manufactured and agricultural goods, as well as bulk energy and retail products. From liquefied natural gas to automobiles to corn, the MTS drives America's economy and delivers vital goods to and from factories, farms, homes, and businesses. With approximately 360 sea and river ports that handle more than \$1.3 trillion in annual cargo, our Nation is critically dependent on a safe, secure, and efficient MTS.⁵

Cyber technology is essential to the operation and efficient functioning of the Nation's maritime critical infrastructure. Computer systems are critical for efficient port operations. They operate pumps, machinery, vessel propulsion and navigation systems; monitor and control safety and environmental systems; operate security cameras, gates, and communication systems; track and control container cargo movements; and enable vessel operators to control ballast water and other ship-stability systems with precision and safety.

INFORMATION SECURITY INCIDENTS:

FY2014 Incidents Reported by Government Agencies by Category



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal year 2014. | GAO-15-573T

⁵ Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity. *Government Accountability Office, GAO Report: GAO-14-459*, pg. 4-7, June 2014. Retrieved from: <http://www.gao.gov/assets/670/663828.pdf>.

The U.S. Coast Guard has a long-standing mission of protecting America's maritime critical infrastructure, and the people who work on and live near the water. The Maritime Transportation Security Act (MTSA)⁶ requires the Coast Guard to prevent and respond to transportation security incidents, which are events that could result in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.⁷ To this end, the Coast Guard conducts boardings and inspections of vessels and facilities, establishes and enforces safety, security, and environmental protection standards, and monitors and patrols America's waters and waterfronts. These activities serve to detect anomalies, deter dangerous or threatening activities, and respond to incidents and attacks.

In 2014, a Government Accountability Office report on maritime critical infrastructure protection highlighted the importance of addressing port cybersecurity to ensure ports remain operational to the maximum extent possible. The report made several recommendations related to the assessment of cyber-related risks, including using cyber-risk assessment results to inform maritime security guidance.⁸

Evolving Cyber Strategy, Policy, and Law

In the U.S., the rapid growth and evolution of cyber technology has continually challenged our Executive, Legislative, and Judicial branches of government.

- Although Executive strategies to address cyber-related security issues have been articulated in over a dozen strategy-related documents since 2000, "...no integrated, overarching strategy has been developed that synthesizes these documents to provide a comprehensive description of the current strategy..."⁹ Moreover, the strategic priorities in these documents have often been revised due to changing circumstances, and have frequently assigned new responsibilities to various organizations.¹⁰
- In December of 2014, Congress passed five cybersecurity-related bills which were signed into law by the President. These bills were the first cybersecurity legislation passed by Congress since the E-Government Act of 2002 and the Federal Information Security Management Act of 2002 (also known as FISMA) were enacted. The laws of 2014 will have broad implications for government agencies and private industry in the years ahead. Most recently, Congress also created the House Subcommittee on Information Technology, which many believe will lead to more frequent and comprehensive cyber legislation in the future.¹¹
- In the Judiciary, many constitutional issues remain open to future interpretation, including issues related to government cyber authorities and activities, legal questions surrounding private sector liability in the management of cybersecurity issues, and constitutional expectations of privacy in cyberspace.

⁶ Maritime Transportation Act of 2002, *Public Law 107-295*, Nov. 25, 2002.

⁷ Executive Order 13636 – Improving Critical Infrastructure Cybersecurity Section 10(a) and 10(b) Report on the United States Coast Guard and Maritime Critical Infrastructure Cyber Security Standards. Retrieved from:

http://www.dhs.gov/sites/default/files/publications/EO%2013636%20Section%2010%28a_b%29%20Report%20for%20USCG_Final.pdf

⁸ Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity. *Government Accountability Office, GAO Report: GAO-14-459*, June 2014. Retrieved from: <http://www.gao.gov/assets/670/663828.pdf>.

⁹ Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented, *GAO Report: GAO-13-187*, pg. 19, February 2013. Retrieved from: <http://www.gao.gov/assets/660/652170.pdf>.

¹⁰ Ibid.

¹¹ Patel, R. "President Obama Signs Five Cybersecurity Bills Into Law." *ZwillGen Blog*, December, 2014. Retrieved from: <http://blog.zwillgen.com/2014/12/29/president-obama-signs-five-cybersecurity-bills-law/>

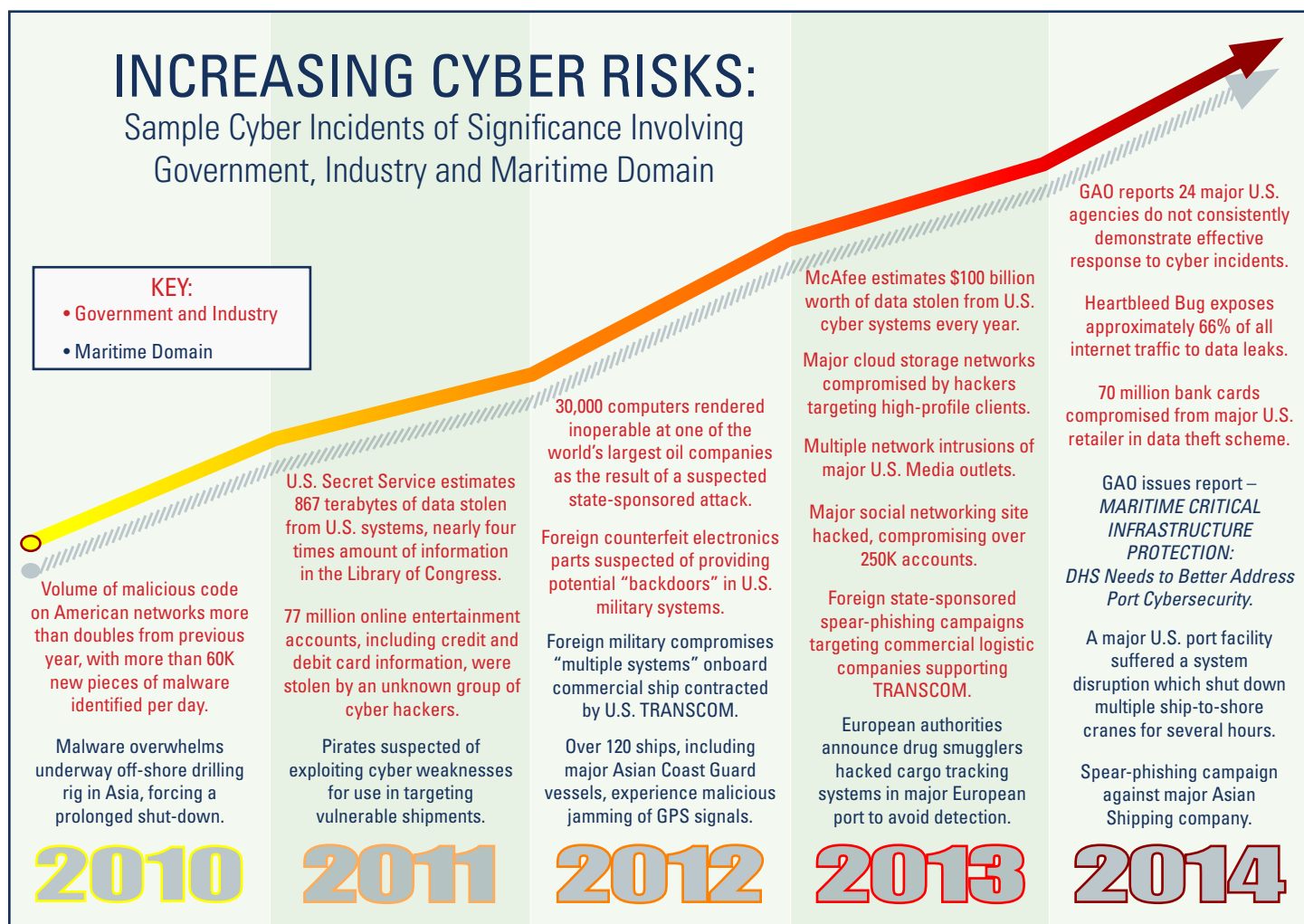
Effective strategic efforts to mitigate the risks in the modern cyber domain must account for a continually changing landscape of strategy, policy, and law. Among other things, these realities will require adaptive strategic approaches that allow for the adjustment of priorities and activities more rapidly than traditional strategic planning cycles have typically supported.

While the emerging cyber domain requires an innovative and adaptive approach, the Coast Guard will always uphold the highest traditions of protecting civil liberties. The Coast Guard bears the responsibility for conducting cyber operations while simultaneously protecting privacy interests, as recognized by applicable executive, legislative, and judicial authority. The imperative to protect the privacy and civil liberties of individuals, preserve business confidentiality, and safeguard sensitive information must always govern the Coast Guard's cyber-related operations and activities.

Manifest Threat – Indicators of Growing Risk

INTERPOL identifies cybercrime as one of the fastest growing areas of crime where more criminals are exploiting the speed, convenience, and anonymity of modern technology to commit a diverse range of criminal activities. These crimes include attacks against computer data and systems, identity and intellectual property theft, fraud, the penetration of critical infrastructure networks, and the deployment of malware, Botnets, and email scams.¹²

Threats in cyberspace, particularly to the maritime community and transportation sector, are real and growing.



12 INTERPOL. (2014). Cybercrime. Retrieved from <http://www.interpol.int/crime-areas/Cybercrime/Cybercrime>.





IV.

BACKGROUND:

U.S. Coast Guard and Cyberspace Operations

The U.S. Coast Guard possesses unique federal authorities in cyberspace. As a law enforcement and regulatory agency that is both a military service and formal member of the U.S. Intelligence Community, the Coast Guard is uniquely positioned to address a broad spectrum of federal cyber activities. These authorities and responsibilities span the .mil, .gov, and .com domains.

Like most federal agencies, the Coast Guard is responsible for defending its information and communications systems and networks. The Coast Guard monitors its computer networks for malicious or anomalous activity, and takes steps to mitigate the vulnerabilities and consequences of malicious cyber activity. Coast Guard networks are part of the Department of Defense's (DOD) Information Network and are subject to compliance with DOD information assurance policies on network security. The Coast Guard also uses National Security Systems, which are subject to the regulations that govern the Intelligence Community.

Most of the critical cyber infrastructure in America's ports is owned and operated by private companies or local governments. The Department of Homeland Security (DHS), through the National Cybersecurity and Communications Integration Center (NCCIC), is responsible for overseeing the protection of federal civilian agencies in cyberspace. The NCCIC is the central civilian portal (public-private partnership) for near-real-time cyber threat indicator sharing. It is a 24x7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. The NCCIC shares information among the public and private sectors to provide greater understanding of cybersecurity and communications situation awareness of vulnerabilities, intrusions, incidents, mitigation, and recovery actions. Working with Sector Specific Agencies (SSAs), the NCCIC oversees the federal response to cyber emergencies or events of national significance that threaten the Nation's critical infrastructure and key resources.

The Coast Guard is the SSA responsible for the Maritime Transportation Mode of the Transportation Systems Sector under the National Infrastructure Protection Plan (NIPP), which directs the Coast Guard to protect the Maritime Transportation System (MTS) from cyber threats. The Coast Guard promotes MTS by encouraging MTS members to conduct risk assessments. In accordance with the Maritime Transportation Security Act, the Coast Guard is charged with



preventing transportation security incidents, which are defined as incidents that can lead to loss of life, environmental damage, transportation system disruption, or economic disruption to a particular area.

The Federal Bureau of Investigation (FBI) is the lead federal agency for investigating most malicious cyber activity and cybercrimes. The FBI heads the National Cyber Investigative Joint Task Force, an interagency organization that serves as the focal point for all government agencies to coordinate, integrate, and share information related to all domestic cyber threat investigations. Other federal law enforcement agencies investigate cybercrimes committed within their jurisdictions, and all federal law enforcement agencies use cyber means to conduct criminal investigations and preserve evidence from digital systems.

As a law enforcement agency, the Coast Guard conducts criminal investigations of illegal activity in the maritime domain and within the service itself. The Coast Guard Criminal Investigative Service (CGIS) seizes and exploits digital information systems and conducts legally sanctioned cyber activities to preserve evidence of illegal activity in accordance with federal legal standards. CGIS conducts or supports investigations into criminal cyber activity targeting or originating in Coast Guard networks or by uniformed members of the Coast Guard. CGIS, when appropriate, coordinates with and assists other federal, state, local, tribal, and territorial, as well as foreign law enforcement agency cyber investigations, and maintains a full-time presence in the National Cyber Investigative Joint Task Force.

The U.S. Intelligence Community (IC) is responsible for providing and securing U.S. national security systems, information systems, and networks that are used for intelligence activities and military command and control or weapons systems. The IC also conducts cyber collection—the collection of foreign intelligence from computers, information or communications systems, or networks—and develops cyber intelligence, intelligence regarding foreign intent or capability to engage in malicious cyber activity, as well as estimates on the potential risk of such activity to the United States. IC counterintelligence (CI) elements are responsible for identifying, deceiving, exploiting, disrupting, countering, or neutralizing malicious cyber activity by foreign powers, organizations, persons, their agents, or international terrorist organizations. The CI cyber mission includes countering threats to the U.S. Government supply chain and threats from trusted insiders.

Coast Guard Intelligence collects, processes, analyzes, and disseminates foreign intelligence information and conducts all-source collection and analysis of foreign cyber threats to Coast Guard and Maritime Transportation Sector networks. The Coast Guard Counterintelligence Service conducts investigations and operations to identify and prevent foreign intelligence service efforts to exploit Coast Guard networks and systems. They also analyze and manage risks to the information and communications supply chain.

DOD is responsible for defending their networks, deterring foreign malicious cyber activity targeting the United States, and, when appropriate, taking decisive action through cyberspace in defense of the nation. Within DOD, U.S. Cyber Command (USCYBERCOM) and the service cyber components (e.g., Coast Guard CYBERCOM) plan, coordinate, integrate, synchronize, and conduct activities to direct the operations and defense of DOD information networks. When authorized, they conduct full-spectrum military cyberspace operations in order to enable actions in all warfighting domains, ensure U.S./Allied freedom of action in cyberspace, and deny the same to all adversaries. The Coast Guard is a uniformed military service that operates in the .mil domain as part of the DOD Information Networks (DODIN), and is responsible for defending information networks and systems under the direction of USCYBERCOM.







V.

STRATEGIC PRIORITY: *Defending Cyberspace*

Coast Guard cyberspace consists of IT systems and networks that are essential to the Service's overall mission success. Threats to these systems and networks have been growing in number and complexity, and will continue to do so for the foreseeable future. Adversaries are extremely sophisticated and employ significant resources. Their persistent and growing assault on Coast Guard cyberspace drains resources, restricts the ability to operate, and has the potential to render the Service incapable of providing for the safety, security, and stewardship of the Nation's waters.

To ensure the Coast Guard is fully capable of performing its essential missions for the Nation, the Service will employ a three-pronged approach. Specifically, the Coast Guard will defend its cyberspace by identifying and hardening systems and networks, understanding and countering cyber threats, and increasing operational resilience.

Goal 1. *Identify and Harden Systems and Networks:* Critical Coast Guard systems are under constant threat from both foreign and domestic actors intent on stealing data or disrupting networks and systems. To reduce the risk from malicious cyber activity, the Coast Guard will improve situational awareness of network operations, and appropriately harden systems against cyber threats.

Objective 1. *Manage Risk:* The Coast Guard must make the best possible use of scarce resources by conducting risk assessments that prioritize internal security measures where they are necessary, and continually evaluate best mitigation options in the context of effectiveness and cost. To achieve this, the Coast Guard will:

- Recognize and understand dependence on cyberspace to assess and manage organizational and operational risks and prioritize investments.
- Foster interagency and inter-departmental partnerships to leverage existing and emerging capabilities.
- Use intelligence to prioritize and focus implementation of risk mitigation and risk reduction actions such as implementation of redundant systems or diverse network paths.
- Continuously monitor and assess the effectiveness of risk mitigation and risk reduction actions to manage vulnerabilities.

Objective 2. *Integrate Cybersecurity into System Planning and Acquisition:*

Cybersecurity must become a fundamental planning consideration for every IT system development or acquisition effort, which addresses resource requirements for recurring budget cycles. To accomplish these goals, the Coast Guard will:

- Understand and manage supply-chain risks across the entire lifecycle of products, systems, and services. Develop acquisition policies and practices that encourage best practices for supply-chain security and risk management.
- Increase security and promote efficiencies in defensive cyberspace operations by continuing alignment with the Joint Information Environment (JIE) and its Single Security Architecture.
- Improve training and education of technology professionals, allowing them to design, build, and operate IT systems that are fundamentally secure and resilient.

Goal 2. *Understand and Counter Cyber Threats:* Defensive cyberspace operations must be informed by timely intelligence and threat indicators, and by vulnerability information from DOD, DHS, and other sources. Cyberspace defensive actions are prioritized and focused through on-time, on-target intelligence.

Objective 1. *Develop the Cyber Workforce:* A professional and technically proficient cyber workforce is essential in the rapidly changing environment of cyberspace. To develop the Service's cyber workforce, the Coast Guard will:

- Recruit, educate, train, and retain agile cyber professionals that thrive in technology-rich cyberspace operations.
- Partner with DOD, DHS, and academia to ensure cutting-edge training and education that remains abreast of technological developments.

Objective 2. *Implement an Efficient and Effective Cyber Intelligence Cycle:*

The Coast Guard must optimize and accelerate intelligence collection, analysis and fusion, dissemination, and feedback functions, to ensure adequate defense of cyberspace. To implement an efficient and effective cyber intelligence cycle, the Coast Guard will:

- Leverage appropriate intelligence collection efforts against illicit cyberspace actors to facilitate cyberspace defense.
- Provide timely all-source indications and warnings, and fused analysis that identifies adversaries, threats, and vulnerabilities presenting cybersecurity risks to Coast Guard operations.
- Facilitate the distribution and exchange of threat information with stakeholders across the Coast Guard and U.S. Government security enterprise tailored for specific intelligence customers at the appropriate security level.

Objective 3. *Conduct Intelligence-driven Cyberspace Defense:* Intelligence must drive operational decisions and actions of cyberspace defense operators. To accomplish this, the Coast Guard will:

- Conduct effective cybersecurity investigations and forensics analysis to determine the methods and paths of malicious activity; determine the impact to infrastructure; provide evidence for prosecution; inform the development of countermeasures; inform defensive operations.

- Leverage open source, DOD, and DHS threat intelligence and indicators to focus limited resources on vulnerabilities and threats that present the highest risk to Coast Guard missions.

Goal 3. *Increase Operational Resilience:* Operational resilience requires that information resources are trustworthy, operational commanders are prepared for degradation or loss of information resources and network operators and defenders have the means to prevail in the face of adverse events.

Objective 1: *Ensure Mission-focused Cyberspace Operations:* Develop capability to actively defend against cyber threats that could potentially degrade operational capability, and appropriately prioritize recovery efforts after cyber incidents. To achieve this goal, the Coast Guard will:

- Identify IT systems, networks, and data that are critical to Coast Guard missions and understand vulnerabilities, critical dependencies, and the potential for cascading disruptions on critical infrastructure.
- Build strong partnerships among Coast Guard security enterprise stakeholders for rapid restoration of critical information infrastructure in the event of system failure or compromise, while maintaining support to ongoing missions.
- Allocate cyberspace defense resources dynamically as needed to sustain operations while addressing cyber incidents.
- Routinely conduct exercises to test contingency plans and capture lessons learned, and test plans to sustain operations in the face of degraded capabilities.

Objective 2. *Incorporate Cybersecurity into Coast Guard Culture:* Almost every aspect of Coast Guard operations is dependent upon reliable and trustworthy IT systems and infrastructure. The Coast Guard must make consistent adherence to IT security policies and recognize cyber hygiene as one of its highest priorities. To this end, the Coast Guard will:

- Recognize and understand our dependence on cyberspace and demonstrate that understanding by treating our information systems and networks as a mission critical asset.
- Deter malicious insiders and advance individual accountability by ensuring that members of the workforce are considered for administrative or judicial sanctions if they knowingly, willfully, or negligently compromise the security of Coast Guard information systems or violate information system security policies.
- Ensure mission success through the development of incident contingency plans, to include plans to continue operations in the face of substantially degraded information systems and networks.
- Improve training and education of all Coast Guard personnel (including non-traditionally IT-focused professionals), empowering the workforce to effectively operate IT systems and tools to maximize operational capabilities, while simultaneously ensuring Coast Guard information systems remain fundamentally secure and resilient.





VI.

STRATEGIC PRIORITY:

Enabling Operations

To operate effectively within the cyber domain, the Coast Guard must develop and leverage a diverse set of cyber capabilities and authorities. Cyberspace operations, both inside and outside Coast Guard information and communications networks and systems, can help detect, deter, disable, and defeat adversaries. Coast Guard leaders must recognize that cyber capabilities are a critical enabler of success across all missions, and ensure that these capabilities are leveraged by commanders and decision-makers at all levels.

In keeping with its long history of protecting and respecting U.S. citizens, the Coast Guard will always act within the confines of governing law and policy of our free Nation, and will always operate with the highest regard to the civil liberties and rights of all citizens. The Coast Guard will leverage approaches, processes, tools, and authorities that will maximize our effectiveness amongst—and against—diverse and sophisticated adversaries in the cyber domain, while upholding the Service’s legacy of respect for the recognized freedoms of individuals. With the diversity of roles derived from many statutory authorities—an armed service, law enforcement agency, regulatory agency, and Intelligence Community member—the Coast Guard is in a unique position to provide cyber operational capabilities, as well as intelligence and law enforcement support to achieve all strategic priorities.

Goal 1: *Incorporate Cyberspace Operations into Mission Planning and Execution:*

In today’s operating environment, awareness of cyber capabilities and opportunities to support Coast Guard operations is crucial for mission success. The Coast Guard workforce must be familiar with cyberspace capabilities and operations and planners and commanders must incorporate cyber considerations in all aspects of operational planning.

Objective 1. *Integrate Cyber Awareness:* All Coast Guard elements operate in cyberspace. As such, the Coast Guard will foster collaboration across cyber activities, as well as with other federal and international partners in a seamless, efficient, and effective manner. Cyber capabilities must be a fundamental consideration in the formation of policy, plans, and strategy. To help integrate cyber awareness, the Coast Guard will:

- Develop and implement doctrine and processes to coordinate cyber activities among the cybersecurity, intelligence, counterintelligence, law enforcement, and regulatory elements within the Coast Guard to reduce risk and maximize effective mission execution through de-confliction and economy of effort.

- Integrate Coast Guard cyber activities as necessary with appropriate federal intelligence, counterintelligence, law enforcement, maritime industry, and military organizations to best build cyber expertise, subject to applicable law and regulation.

Objective 2. *Build Capability and Capacity:* Coast Guard operators must understand the fundamentals of cybersecurity and cyberspace operations. This is critical to enhancing the Coast Guard's ability to guard against cyber adversaries, counter those adversaries in cyberspace, and support the cybersecurity of the Maritime Transportation Sector. Cyber education and training must be a major component of core workforce skills and competencies. The Coast Guard will build a force of cyberspace operators capable of ensuring freedom of action in this complicated operational domain, while upholding the privacy and civil liberties of citizens. To achieve this, the Coast Guard will:

- Develop and implement foundational cyber awareness programs for all Service members and civilians, or any person with authorized access to Coast Guard systems. This begins with accession and continues throughout members' service.
- Develop a career path for Coast Guard cyberspace operations personnel to include recruitment, training, and retention, to create a professional cadre with specialized skills in cybersecurity, cyber intelligence, cyber law enforcement missions, cyber support to critical infrastructure, and cyber effects* operations.
- Manage risk across the enterprise by developing an appropriately sized cyberspace operations workforce capable of defending Coast Guard cyberspace and conducting operations in support of Coast Guard missions.

Goal 2: *Deliver Cyber Capabilities to Enhance All Missions:* Cyber intelligence and criminal investigations are vital to shaping effective Coast Guard decision-making and must inform policy, strategy, operations, and tactics. Cyberspace operations are conducted to enhance the performance of missions and cybersecurity. These operations will improve mission success by producing intelligence, via the cyberspace operation itself, or through the byproduct of a continuous intelligence cycle.

Objective 1. *Intelligence Support to Cyberspace Operations:* Intelligence is most valuable when it is relevant, actionable, and timely, while delivered in a practical manner. The Coast Guard must use intelligence and investigative capabilities, and leverage the Intelligence Community (IC) and law enforcement partners, to enhance mission performance. To this end, the Coast Guard will:

- Partner with Department of Defense (DOD), Department of Homeland Security (DHS), and others to build, progress, and perpetuate a broad and deep expertise in all-source cyber intelligence for service utility, while being a proactive contributor to the greater community needs.
- Develop information-sharing and safeguarding guidelines consistent with federal policy to ensure that cyber threat indicators and criminal investigative information can be shared in a timely manner internally, as well as with international, federal, state, local, tribal, and territorial partners when appropriate.
- Develop policies and guidelines for ensuring the rapid dissemination of cyber threat indicators to maritime partners and stakeholders to enhance the safety, security, and resiliency of the Maritime Transportation System.

Objective 2. *Cyber Support to Operations:* All Coast Guard mission priorities are impacted by developments in cyberspace. The Coast Guard's ability to conduct missions effectively requires clear understanding of threats. Cyber capabilities must inform and support all Coast Guard operations. Operational commanders and operational planners must incorporate cyber support as part of their operational planning. To accomplish this objective, the Coast Guard will:

- Develop strong cyber intelligence, surveillance, and reconnaissance capabilities to support to Coast Guard missions.
- Leverage partnerships with DOD and DHS. Evaluate rapidly evolving cyber technologies and tools for potential use in supporting operational objectives for Coast Guard missions.
- Integrate cyber activities into Coast Guard operational planning and operations at appropriate command echelons throughout the service.
- Develop coordinated courses of action to support specific cyber operations, or response to cyber threats, by leveraging interagency operational and intelligence partnerships. This includes coordinated requirements for national cyber-related intelligence and operational resources.
- Evaluate the need for an operational cyber policy review board, which will regularly assess evolving changes in law and policy against the backdrop of Coast Guard operations and practice, ensuring checks and balances are maintained throughout the operational cycle.





**U.S.
COAST
GUARD**



VII.

STRATEGIC PRIORITY:

Protecting Infrastructure

Maritime Critical Infrastructure includes the ports, facilities, vessels, and related systems that facilitate trade within the U.S., support national defense and homeland security objectives, and connect the Nation to the global supply chain. This infrastructure, in combination with the people who operate it, constitutes the Maritime Transportation System (MTS). American security and prosperity depends upon a safe, secure, and efficient MTS.

It is the stated policy goal of the United States to strengthen the security and resilience of the Nation's critical infrastructure, and to maintain a cyber environment that encourages efficiency, innovation, economic prosperity, while promoting safety, security, business confidentiality, privacy, and civil liberties.¹³ Working with the Department of Homeland Security (DHS), the Coast Guard will achieve these goals through collaboration with the owners and operators of critical infrastructure to improve cybersecurity information sharing and develop and implement risk-based standards.

The U.S. Coast Guard has long defended maritime critical infrastructure and the MTS from attack, accident, and natural disaster. Employing patrols, inspections, exercises, and other activities, the Coast Guard works with the private sector to reduce risk and remain ready for incidents and attacks.

Cyber-related risks are a growing portion of the vulnerabilities facing the MTS. Vessel and facility operators use computers and cyber-dependent technologies for navigation, communications, engineering, cargo, ballast, safety, environmental control, and many other purposes. Collectively these technologies enable the MTS to operate with an impressive record of reliability and at a capacity that drives the U.S. economy and supports national defense, homeland security, and related needs.

While these cyber systems create benefits, they also introduce risk. Exploitation, misuse, or failure of cyber systems could cause injury or death, harm the marine environment, or disrupt vital trade activity. Even a temporary or partial disruption of MTS operations could have serious consequences for the local, regional, national, and even global economy. Three quarters of our Nation's commerce passes through our ports and waterways,¹⁴ including coastal ports, the Great Lakes, and the Western Rivers.

¹³ Executive Order 13636, Feb. 12, 2013, Improving Critical Infrastructure Cybersecurity. Retrieved from: <http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf>.

¹⁴ U.S. Dept. of Transportation, Research & Innovative Technology Admin., Bureau of Transportation Statistics. Transportation Statistics Annual Report 2012. Available at <http://www.rita.dot.gov>.

To address these risks, the Coast Guard, the marine industry, and other stakeholders will work to identify appropriate cyber standards and include them in existing safety and security compliance activities for vessels and facilities. The Coast Guard's operating model is to prevent adverse consequences whenever possible, and to respond to mitigate the consequences of those events when they do occur. Both prevention and response operations play important roles in protecting maritime critical infrastructure in cyberspace.

Goal 1. *Risk Assessment – Promote Cyber Risk Awareness and Management:*

The Coast Guard will incorporate cybersecurity into aspects of maritime operations in order to reduce the risk to the MTS and to continue to protect the nation's maritime critical infrastructure and the American people.

Objective 1. *Improve Port-Wide Cybersecurity Risk Assessment Tools and*

Methodologies: The Coast Guard will leverage risk assessment tools to help defend maritime critical infrastructure. To accomplish this goal, the Coast Guard will:

- Incorporate cybersecurity into the risk assessments completed by Area Maritime Security Committees.
- Modify Maritime Security Risk Assessment Model (MSRAM) to incorporate cyber risks, or identify a similar tool that performs the same function.
- Leverage grant funding and research and development capacity to evaluate cyber risks in the maritime domain.
- Identify existing cybersecurity risk assessment tools, and where appropriate, adapt them for Coast Guard use and share them with the maritime industry.

Objective 2. *Improve Cybersecurity Information Sharing:* The Coast Guard will work with partners and stakeholders to establish information sharing protocols on threats to maritime infrastructure. To achieve this objective, the Coast Guard will:

- Work with the maritime industry, Area Maritime Security Committees, DHS, and other stakeholders, evaluating the feasibility of establishing an Information Sharing and Analysis Center (ISAC) to share cybersecurity related information with the maritime industry.
- Establish Memoranda of Understanding with DHS' National Cybersecurity and Communications Integration Center (NCCIC) and other organizations to clarify and facilitate information sharing processes related to cybersecurity risks.
- Continue to support the information sharing and related objectives of the National Infrastructure Protection Plan. Lead the Maritime Government Coordinating Council; participate in other sectors' Government and Sector Coordinating Councils.
- Continue to work with Transport Canada to compare and share best practices on cybersecurity risk analysis methodologies, and to share information on emerging cyber threats. Support information sharing efforts on a multi-lateral approach through the International Maritime Organization (IMO) and other fora.
- Continue to build interagency partnerships to support and improve the MTS cybersecurity through participation on the U.S. Committee on the Maritime Transportation System (CMTS).

Goal 2. Prevention – Reduce Cybersecurity Vulnerabilities in the MTS: Understanding the vulnerabilities associated with cyber systems enables the Coast Guard and the marine industry to take appropriate steps to reduce the risk to maritime cyber critical infrastructure from attack, exploitation, failure, or misuse.

Objective 1. Reduce Cyber Vulnerability for Vessels and Facilities: The Coast Guard will identify and incorporate appropriate standards to reduce the vulnerability of cyber-dependent systems to attack, exploitation, failure, or misuse that could cause or contribute to a Transportation Security Incident,* or other adverse impacts subject to Coast Guard authority. To help reduce cyber-related vulnerability, the Coast Guard will:

- Develop guidance for commercial vessel and waterfront facility operators on how to identify and evaluate their cybersecurity-related vulnerabilities. Incorporate this risk information into existing vessel and facility security assessments, or other appropriate management regimes, conducted by private industry and port authorities.
- Improve resilience in the MTS to cyber-related events by promoting response and recovery planning and other actions to reduce the consequences of cyber events.
- Work with international organizations, as well as industry and technical associations, to identify existing cybersecurity standards appropriate to systems commonly used in the international and domestic marine industry.
- Review design and operating standards for Coast Guard required equipment to determine those where accepted cybersecurity standards could improve the security and reliability of the systems.
- Work with the IMO to develop global maritime cyber prevention and response protocols.
- Incorporate cybersecurity into existing enforcement and compliance programs.

Objective 2. Incorporate Cybersecurity into Training and Education

Requirements: Educated crewmembers, facility workers, and the Coast Guard personnel who operate alongside them, are vital to reducing the vulnerability of cyber systems within the MTS. The Coast Guard will ensure that mariners and facility personnel who operate vital cyber systems are properly trained to use the systems safely, understand the risks, and can detect anomalous activities. To this end, the Coast Guard will:

- In coordination with the International Maritime Organization, incorporate cybersecurity into required training for vessel and facility security officers.
- Incorporate cybersecurity into the requirements for Coast Guard-issued credentials.
- Work with the United States Coast Guard Academy, merchant marine academies, and training programs to incorporate cybersecurity into course curricula.





VIII.

Ensuring Long-Term Success

There are several cross-cutting enabling objectives that must be considered during implementation of this strategy. While not exhaustive, the following concepts are especially important to ensure the Coast Guard meets its strategic priorities in the cyber domain.

Recognize Cyberspace as an Operational Domain:

The Coast Guard must promote a culture that recognizes the importance of cyberspace operations, which has become just as important as operations in physical domains. Operational commands at all levels must develop objectives and expectations for cyberspace operations within their areas of responsibility, and ensure that the cyber component is considered in all mission planning and execution. Additionally, every Coast Guardsman—enlisted, officer, civilian, reservist, or auxiliary—must learn his or her roles and responsibilities for ensuring the Coast Guard remains secure and is able to maximize use of cyberspace to execute all missions.

Develop Operational Cyber Guidance and Define Mission Space:

The Coast Guard must develop clear guidelines as to when and how personnel will conduct operations in cyberspace, and how to coordinate and align our operations with other government and private sector organizations. The Coast Guard must also develop rules of engagement in cyberspace that are consistent with statutory authorities and clarify operating parameters. The Coast Guard is a federal law enforcement and regulatory agency, a member of the Intelligence Community, and an armed service, with legal authority to conduct operations in support of its statutory missions. The Coast Guard must clearly articulate legal authorities and responsibilities for cyber operations amidst continually evolving cyber policy and law. As conditions change, the Coast Guard must adapt cyber programs and operations to ensure optimal mission performance while fully complying with applicable policy and law.

Leverage Partnerships:

While the Coast Guard has a unique set of authorities to conduct cyber operations in support of missions, it is a small agency with limited resources. To operate effectively in cyberspace, the Coast Guard must work with partners across the Federal Government; in foreign governments; at the state, local, tribal, and territorial levels; and in the private sector. At the federal level, the Coast Guard must align capabilities and coordinate cyber operations with the Department of Homeland Security (DHS) to ensure optimal unity of effort. The Coast Guard must also work closely with the Federal Bureau of Investigation, the National Security Agency, and U.S. Cyber Command, and other federal departments and agencies. The Service must train its personnel to conduct operations to the applicable standards of all partners, and where appropriate, integrate

Coast Guard cyber personnel into the partner agencies to ensure participation and coordination with their cyber activities. The Coast Guard must also foster close relations with private sector members of the Maritime Transportation Sector to understand their vulnerabilities and support their cybersecurity efforts. Additionally, the Service must work with academia—leveraging its special relationship with the United States Coast Guard Academy, as well as research and development centers, and the information and communications technology sector—to capitalize on their unique knowledge of trends in cyberspace that will impact Coast Guard missions.

Communicate in Real-Time:

Timely information-sharing is the lifeblood of cooperative relationships. Providing effective cyber support to Coast Guard operations and critical infrastructure cybersecurity requires a careful balance between the rapid sharing and careful safeguarding of information. Information derived from Coast Guard and national intelligence sources and methods or from law enforcement and network defense investigations must be made available to Coast Guard operational elements and Maritime Transportation Sector partners in a timely and relevant manner. Information shared with operators and partners must be in formats that are useful to the customer, and at classification levels that they can act upon. The Coast Guard must also develop information sharing procedures to ensure that cyber information necessary to the performance of critical missions will be shared with appropriate partners while being protected from unauthorized disclosure. The Coast Guard must also work with DHS and Maritime Transportation Sector partners to develop procedures for receiving, using, and protecting critical private sector information on cyber threats and vulnerabilities in the Maritime Transportation System (MTS).

Organize for Success:

The Coast Guard's cyber cadre has multiple missions—cybersecurity, criminal investigations, intelligence collection and analysis, counterintelligence, regulatory direction and support to critical infrastructure cybersecurity, and cyber effects* operations—that are spread out across many organizations and geographic locations throughout the service. This dispersed activity requires an agile and adaptive command structure to ensure unity of effort in cyberspace. The Coast Guard must develop a command and control structure that ensures that the diverse cyber elements within the service coordinate, deconflict, and cooperate with each other, and align their activities with Coast Guard tactical and strategic priorities. This will include creating policies and processes to facilitate requests for and approval of cyber support to operations, standards for planning and conducting cyber operations, and means of recording and learning from Coast Guard cyberspace operations.

Build a Cyber Workforce:

The Coast Guard must identify the personnel requirements and skill sets needed to develop a specialized cyber cadre, and then create policies and opportunities for recruiting, training, and retaining them. As cyberspace gains recognition as an operating domain, “cyber-operators” will be equally important to Coast Guard operations as all other operational specialties. The Service must ensure that our cyber cadre has incentives to continue enhancing their skills and opportunities to advance professionally within the cyber field. Cyber personnel must have the opportunity to expand their capabilities by cross-training and serving in the full gamut of Coast Guard cyber elements, in cybersecurity, policy, intelligence, counterintelligence, law enforcement, regulatory, and serve in air, land, and sea domains. In addition to developing a specialized cyber force, the Coast Guard must also ensure the entire workforce develops the necessary skills and knowledge to effectively operate in the cyber domain, while also continuously acquiring practices to ensure Coast Guard systems remain safe and secure.

Invest in the Future:

The information and communications technology sector is evolving rapidly. The Coast Guard must keep up with technological developments in cyberspace if it is to manage emerging risks and exploit new opportunities. Coast Guard acquisitions and information technology management practices must be agile and adaptive to changes in the information and communications technology sector. The Coast Guard must enhance service capabilities by investing in cyber research and development to foresee and shape the future operating environment.







IX.

Conclusion

Cyber technologies have ushered in an unprecedented era of progress and efficiency, yet they have also given rise to grave threats and risks. These risks pose significant challenges to Coast Guard readiness and mission performance, and could have devastating impacts to the Maritime Transportation System. Protecting against these threats, and maximizing overall effectiveness as a Service in the modern digital age, will require the Coast Guard to strategically adapt. *First and foremost, the Coast Guard must fully embrace cyberspace as an operational domain.*

This Strategy offers a clear framework for the Coast Guard's plan to operate effectively and efficiently within the cyber domain. It emphasizes three essential strategic priorities: Defending Cyberspace, Enabling Operations, and Protecting Infrastructure. It also outlines a number of critical success factors that will ensure the Service's long-term success.

This strategy will be executed in close coordination with the Department of Homeland Security, Department of Defense, the Intelligence Community, and in consultation with the full range of partners across the whole of government, as well as global and private sector partners. To support long-term success, the Service will build a culture that values cybersecurity and recognizes cyberspace as an operational domain. It must organize, train, and equip its members for the operating environment of today, and well into the future. Most importantly, the Coast Guard will carry on its long tradition of collaboration with partners from across the public and private sectors, both domestically and internationally, to ensure the most effective and efficient possible execution of its missions.

To protect the Nation's most vital and enduring interests in the maritime environment, the Coast Guard must move forward to operate in the cyber domain. The Coast Guard will continue to adapt, as it has done over the last two centuries, to the challenges and opportunities that accompany technological advancements in our operating environment. By employing this strategy, the Coast Guard will effectively protect America's maritime interests in cyberspace, maintain advantage over adversaries, and help maintain the safety, security, and prosperity of the Nation.



Appendix I

Glossary of Key Terms

Access – The ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Adversary – An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Critical Infrastructure – Those 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 debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (*Executive Order 13636, Improving Critical Infrastructure Cybersecurity; February 12, 2013*)

Cyber collection – Intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (*DOD, Joint Publication 3-13*)

Cyber-Dependent Critical Infrastructure – Critical Infrastructure where a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security. (*Executive Order 13636*)

Cyber domain – The operational domain within the information environment consisting of the interdependent networks of information technology, infrastructures and resident data, including the Internet, telecommunications networks, computer systems, embedded processors and controllers that operate in the electromagnetic spectrum, which includes cyberspace operation activities and programs.

Cyber effects – The manipulation, disruption, denial, degradation, or destruction of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

Cyber event – A cybersecurity change that may have an impact on organizational operations, including mission, capabilities, or reputation. (*NIST Cybersecurity Framework v. 1.0*).

Cyber incident – An occurrence that actually or potentially results in adverse consequences to an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Cyber intelligence – The collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, and operational activities and indicators; their impact or potential effects on national security, information systems, infrastructure, and data; and insight into the components, structures, use, and vulnerabilities of foreign information systems. (*Office of the Director of National Intelligence, National Intelligence Strategy 2014*)

Cyber investigation – A systematic and formal inquiry into a qualified threat or incident using a full range of criminal investigative tools, including but not limited to interview techniques, surveillance, and digital forensics to determine the events that transpired and to collect evidence. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Cyber or cyberspace operations – The employment of cyberspace capabilities where the primary purpose is to achieve military and/or mission objectives or effects in or through cyberspace. Also, cybersecurity work where a person performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities (*DOD Joint Publication (JP) 3-0, Doctrine for Joint Operations; Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

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. (*U.S. Department of Homeland Security. National Infrastructure Protection Plan, 2013*)

Cybersecurity breach — Unauthorized access to data, applications, services, networks and/or devices, by-passing their underlying security mechanisms. A cybersecurity breach that may rise to the level of a reportable Maritime Transportation Security Act (MTSA) security breach occurs when an individual, an entity, or an application illegitimately enters a private or confidential Information Technology perimeter of a MTSA-regulated facility or vessel, Maritime Critical Infrastructure/Key Resources, or industrial control system such as Supervisory Control and Data Acquisition systems, including but not limited to terminal operating systems, global positioning systems, and cargo management systems. (*U.S. Coast Guard Atlantic Area Commanders Intent: Advancing Knowledge of Cyber Security Trends and Threats to the Maritime Transportation System (MTS), 4 November 2013; U.S. Coast Guard Pacific Area Commanders' Intent: Cyber Security and the Maritime Transportation System (MTS), 8 November 2013*)

Cyber program — An organization's comprehensive and broad approach to cyber technology, including defensive actions, operations, and oversight.

Cyberspace — The interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computers, information or communications systems, networks, and embedded processors and controllers. (*Source: SUBJECT: U.S. Cyber Operations Policy (U); National Security Presidential Directive (NSPD) 54/Homeland Security Presidential Directive (HSPD) 23, SUBJECT: Cybersecurity Policy (U); 8 January 2008*)

Cyber technology — the growing body of technical processes, methods, or knowledge that relies upon networks of information and infrastructures, including the Internet, telecommunications networks, computer systems, embedded processors and controllers that operate in the electromagnetic spectrum.

Cyber threat — A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Cyber threat actor — An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Detect (function) — Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Information and communications technology — Technologies that provide access to information through telecommunications, including the Internet, wireless networks, cell phones, and other communications mediums. (*www.techterms.com*)

Information system — Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information and includes: A) computers and computer networks; B) ancillary equipment; C) software, firmware, and related procedures; D) services, including support services; and E) related resources. (*Title 44 U.S. Code section 3532*)

Insider threat — One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Intelligence — Information gathered from various sources used to inform, shape, and make operational decisions. This information is gathered subject to multiple laws and regulations that place limitations upon its use. (*See E.O. 12333, United States intelligence activities. The provisions of Executive Order 12333 of Dec. 4, 1981, appear at 46 FR 59941, 3 CFR, 1981 Comp., p. 200, unless otherwise noted.*)

Intrusion — An unauthorized act of bypassing the security mechanisms of a network or information system. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Malicious cyber activity — Activities, other than those authorized or in accordance with U.S. law, that seek to compromise the confidentiality, integrity, or availability of computers, information or communications systems, physical or virtual infrastructure controlled by computers or information systems, or information thereon.

Mitigation – The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

National security system – Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or any other organization on behalf of an agency, the function, operation, or use of which: A) involves intelligence activities; B) involves cryptologic activities related to national security; C) involves command and control of military forces; D) involves equipment that is an integral part of a weapons system; or E) is critical to the direct fulfillment of military or intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). (*Title 44 U.S. Code section 3532*)

Network defense – The programs, activities, and the use of tools necessary to facilitate them conducted on a computer, network, or information or communications system by the owner or with the consent of the owner and, as appropriate, the users for the primary purpose of protecting 1) that computer, network, or system; 2) data stored on, processed on, or transiting that computer, network, or system; or 3) physical and virtual infrastructure controlled by that computer, network, or system. Network defense does not involve or require accessing or conducting activities on computers, networks, or information or communications systems without authorization from the owners or exceeding access authorized by the owners.

Network resilience – The ability of a network to: (1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged); (2) recover effectively if failure does occur; and (3) scale to meet rapid or unpredictable demands. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Recovery – The activities after an incident to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Response – The activities that address the short-term, direct effects of an incident and may also support short-term recovery. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Risk – The potential for an unwanted or adverse outcome resulting from an incident, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Risk assessment – The appraisal of the risks facing an entity, asset, system, or network, organizational operations, individuals, geographic area, other organizations, or society, and includes determining the extent to which adverse circumstances or events could result in harmful consequences. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Risk Management – The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Shared Situational Awareness – Knowledge and understanding of the current situation which promotes timely, relevant, and accurate assessment of friendly, adversary, and other operations in order to facilitate decision making. (*U.S. Army Field Manual*)

Supply chain – A system of organizations, people, activities, information and resources, for creating and moving products including product components and/or services from suppliers through to their customers. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Transportation Security Incident – A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. In this paragraph, the term “economic disruption” does not include a work stoppage or other employee-related action not related to terrorism and resulting from an employee-employer dispute. (*46 U.S. Code § 70101*)

Unauthorized Access – Any access to an information system or network that violates the owner or operator’s stated security policy. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)

Vulnerability – A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard. (*Department of Homeland Security, National Initiative for Cybersecurity Careers and Studies*)



U.S. COAST GUARD HEADQUARTERS
WASHINGTON, D.C.

CG-DCO-X

www.uscg.mil