

July 2011

DEFENSE
DEPARTMENT
CYBER EFFORTS

DOD Faces
Challenges In Its
Cyber Activities

U.S. Government Accountability Office

GAO90

YEARS

1921-2011

ACCOUNTABILITY ★ INTEGRITY ★ RELIABILITY

Why GAO Did This Study

According to the U.S. Strategic Command, the Department of Defense (DOD) is in the midst of a global cyberspace crisis as foreign nation states and other actors, such as hackers, criminals, terrorists, and activists exploit DOD and other U.S. government computer networks to further a variety of national, ideological, and personal objectives. This report identifies (1) how DOD is organized to address cybersecurity threats; and assesses the extent to which DOD has (2) developed joint doctrine that addresses cyberspace operations; (3) assigned command and control responsibilities; and (4) identified and taken actions to mitigate any key capability gaps involving cyberspace operations. It is an unclassified version of a previously issued classified report. GAO analyzed policies, doctrine, lessons learned, and studies from throughout DOD, commands, and the services involved with DOD's computer network operations and interviewed officials from a wide range of DOD organizations.

What GAO Recommends

GAO recommends that DOD (1) establish a timeframe for deciding on whether to complete a separate joint cyberspace publication and for updating the existing body of joint publications, (2) clarify command and control relationships regarding cyberspace operations and establish a timeframe for issuing the clarified guidance, and (3) more fully assess cyber-specific capability gaps, and (4) develop a plan and funding strategy to address them. DOD agreed with the recommendations.

View [GAO-11-75](#) or key components. For more information, contact Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

DEFENSE DEPARTMENT CYBER EFFORTS

DOD Faces Challenges In Its Cyber Activities

What GAO Found

DOD's organization to address cybersecurity threats is decentralized and spread across various offices, commands, military services, and military agencies. DOD cybersecurity roles and responsibilities are vast and include developing joint policy and guidance and operational functions to protect and defend its computer networks. DOD is taking proactive measures to better address cybersecurity threats, such as developing new organizational structures, led by the establishment of the U.S. Cyber Command, to facilitate the integration of cyberspace operations. However, it is too early to tell if these changes will help DOD better address cybersecurity threats.

Several joint doctrine publications address aspects of cyberspace operations, but DOD officials acknowledge that the discussions are insufficient; and no single joint publication completely addresses cyberspace operations. While at least 16 DOD joint publications discuss cyberspace-related topics and 8 mention "cyberspace operations," none contained a sufficient discussion of cyberspace operations. DOD recognizes the need to develop and update cyber-related joint doctrine and is currently debating the merits of developing a single cyberspace operations joint doctrine publication in addition to updating all existing doctrine. However, there is no timetable for completing the decision-making process or for updates to existing doctrine.

DOD has assigned authorities and responsibilities for implementing cyberspace operations among combatant commands, military services, and defense agencies; however, the supporting relationships necessary to achieve command and control of cyberspace operations remain unclear. In response to a major computer infection, U.S. Strategic Command identified confusion regarding command and control authorities and chains of command because the exploited network fell under the purview of both its own command and a geographic combatant command. Without complete and clearly articulated guidance on command and control responsibilities that is well communicated and practiced with key stakeholders, DOD will have difficulty in achieving command and control of its cyber forces globally and in building unity of effort for carrying out cyberspace operations.

DOD has identified some cyberspace capability gaps, but it has not completed a comprehensive, departmentwide assessment of needed resources, capability gaps, and an implementation plan to address any gaps. For example, U.S. Strategic Command has identified that DOD's cyber workforce is undersized and unprepared to meet the current threat, which is projected to increase significantly over time. While the department's review of some cyberspace capability gaps on cyberspace operations is a step in the right direction, it remains unclear whether these gaps will be addressed since DOD has not conducted a more comprehensive departmentwide assessment of cyber-related capability gaps or established an implementation plan or funding strategy to resolve any gaps that may be identified.

Contents

Letter		1
	Results in Brief	4
	Background	9
	Key Terms for DOD's Cyberspace Domain	15
	Cybersecurity Roles and Responsibilities Are Spread across DOD, and DOD Is Reorganizing to Better Address Cybersecurity Threats	17
	DOD Recognizes the Need to Update Cyber-Related Joint Doctrine and Guidance, but Lacks a Timetable for Completion	26
	Conflicting Guidance and Unclear Responsibilities Have Created Challenges for Command and Control of Cyberspace Operations	34
	DOD Has Identified Some Capability Gaps in Cyber Operations, but Lacks a Comprehensive Assessment of Departmentwide Cyberspace Needs and an Implementation Plan to Address Any Gaps	37
	Conclusions	42
	Recommendations for Executive Action	43
	Agency Comments and Our Evaluation	44
Appendix I	Objectives, Scope, and Methodology	49
Appendix II	DOD Cyber Organizations	53
Appendix III	Cyberspace Defensive Measures and Mechanisms Used by DOD	61
Appendix IV	Audit Community Work in Information Security	68
Appendix V	Comments from the Department of Defense	71
Appendix VI	GAO Contacts and Staff Acknowledgments	74

Tables

Table 1: Sources of Cyber Threats	13
Table 2: Types and Techniques of Cyber Attacks	14
Table 3: Key Terms for DOD Cyberspace	16
Table 4: Examples of DOD Studies Related to Cyber Joint Doctrine	32
Table 5: Office of the Secretary of Defense Cyber-Related Responsibilities and Efforts	53
Table 6: Joint Staff Cyber-Related Responsibilities and Efforts	54
Table 7: Cyber-Related Coordination Forums	55
Table 8: Roles and Responsibilities of U.S. Strategic Command	55
Table 9: Roles and Responsibilities of Combatant Command Network Centers	56
Table 10: Roles and Responsibilities of Service Network Centers	56
Table 11: Cyber Organization of the Military Services as of January 2009	57
Table 12: Roles and Responsibilities of Intelligence Agencies	57
Table 13: Roles and Responsibilities of Defense Criminal Investigative-Related Organizations	58
Table 14: Current or Proposed Cyber Organization of the Military Services	59

Figure

Figure 1: DOD Cyber Organization as of March 2010	18
---	----

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

July 25, 2011

Congressional Requesters

The wealth and strength of the United States make it a target in cyberspace. The U.S. economy and government are the most dependent in the world on the Internet and therefore the most vulnerable to cyber attacks. Information technology powers the U.S. economy and enables almost everything the military does, including command and control of forces, intelligence gathering, and logistical support of troops. According to the President of the United States, the cyber threat is thus one of the most serious national security challenges that the nation faces. The United States confronts a growing array of cyber threats from foreign intelligence services and other actors, including terrorists, criminal groups, and individual hackers, that could compromise our personal and national security. Protecting our digital infrastructure, while safeguarding privacy and civil liberties, is therefore a national security priority, according to U.S. Cyber Command.

In June 2009, the Deputy Secretary of Defense cautioned that the cyber threat is not an emerging or future threat, but one that is already here today. The Department of Defense (DOD) alone depends on 7 million computer devices, linked on over 10,000 networks with satellite gateways and commercial circuits that are composed of innumerable devices and components. The threat to DOD computer networks is thus substantial, and the potential for sabotage and destruction is present. While criminal organizations are a source of concern, foreign governments have more resources and more worrisome motivations. Cyber warfare is attractive to adversaries because it poses a significant threat at a low cost. An adversary does not need an expensive weapons program to conduct damaging attacks; a handful of programmers could cripple an entire information system. Moreover, it is also an attractive weapon to our adversaries because it is difficult to trace the origin of the attack and even more difficult to deter one. According to DOD, a large number of intelligence agencies and foreign militaries are actively trying to penetrate our military networks. These networks are scanned millions of times a day and probed thousands of times a day. Over the past several years, DOD has experienced damaging penetration to these networks. For example, blueprints of weapons systems have already been compromised. Ensuring the security of these networks is therefore critical so DOD can operate securely and confidently not only in the new cyber domain but in the traditional military domains of land, sea, air, and space.

In addition, the recent Quadrennial Defense Review recognized the need for DOD to operate effectively in cyberspace and improve its policy, doctrine, and capabilities to counter threats in cyberspace.¹ It also cautioned that failure to adapt to cyber threats would pose a fundamental risk to DOD's ability to accomplish its missions today.

In prior reports, agency inspector general offices and we have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls.² In the past, we have also reviewed DOD's information security weaknesses in various reports. For example, as early as 1991, we reported on foreign hackers penetrating DOD computer systems between April 1990 and May 1991, as a result of inadequate attention to computer security, such as password management and the lack of technical expertise on the part of some system administrators.³ To see further information on past reports on DOD networks, see appendix IV.

DOD's cyberspace operations encompass both defensive and offensive activities, for which the primary purpose is to achieve military objectives or effects in or through cyberspace. Defensive cyber operations are categorized as computer network defense, which consists of actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. In appendix III we provide further information on DOD tools and programs used to defend its networks. Offensive cyber operations are comprised of two functions: information gathering (or computer network exploitation) and computer network attack. Computer network exploitation is the method by which DOD and the intelligence community gather information on adversaries in and through cyberspace. Computer network attack

¹DOD, *Quadrennial Defense Review Report* (Washington, D.C., February 2010).

²A sample of reports on information security include: GAO, *Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems*, [GAO-05-231](#) (Washington, D.C.: May 13, 2005); GAO, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, [GAO-08-571T](#) (Washington, D.C.: Mar. 12, 2008); GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, [GAO-09-432T](#) (Washington, D.C.: Mar. 10, 2009); and GAO, *Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk*, [GAO-09-661T](#) (Washington, D.C.: May 5, 2009).

³GAO, *Computer Security: Hackers Penetrate DOD Computer Systems*, [GAO/T-IMTEC-92-5](#) (Washington, D.C.: Nov. 20, 1991).

consists of operations through the use of computer networks to disrupt, deny, degrade, or destroy information residing in computers and computer networks or the computers and networks themselves.⁴

In light of worldwide cybersecurity incidents in 2008, you requested that we perform a review focused on DOD's organization and planning of cyberspace operations, including its defensive and offensive efforts to address cyber threats. In prior work, we have examined information security weaknesses in federal government networks, including DOD's networks.⁵ Our objectives for this report were to determine (1) how DOD is organized to address cybersecurity threats; and to assess the extent to which DOD has (2) developed joint doctrine that addresses cyberspace operations across DOD; (3) assigned command and control responsibilities that clearly establish roles between combatant commands and military services; and (4) identified and taken actions to mitigate any key capability gaps involving cyberspace operations. In May 2010, we reported to you on the results of our work in a classified report. This report is an unclassified version of that report. To remove information DOD determined to be classified, this report omits details on DOD cyber-related planning, operations, capabilities, and capability gaps.

To answer the objectives, we reviewed documentation and conducted interviews with DOD officials at the Office of the Secretary of Defense; the Army, the Navy, the Marine Corps, and the Air Force; U.S. Strategic Command; U.S. Central Command; U.S. Pacific Command; U.S. European Command; U.S. Northern Command; U.S. Africa Command; U.S. Joint Forces Command; U.S. Special Operations Command; Joint Staff; the National Security Agency; and other cognizant organizations. To evaluate DOD's organization to address cybersecurity threats, we conducted interviews and analyzed various policies, guidance, and directives relating to organizations involved with the department's computer network operations. We also reviewed documents involving the reorganization and development of new organizations within the Office of the Secretary of Defense, U.S. Strategic Command, the Air Force, and

⁴Although computer network exploitation is an integral part of computer network operations, we focused specifically on computer network attack capabilities.

⁵[GAO-09-661T](#) and GAO, *DOD Information Security: Further Efforts Needed to Fully Implement Statutory Requirements in DOD*, [GAO-03-1037T](#) (Washington, D.C.: July 24, 2003).

the Navy to address cyber threats. To determine the extent to which DOD has developed an overarching joint doctrine that addresses cyberspace operations across DOD, we reviewed and analyzed current joint doctrine publications involving computer network operations and U.S. Joint Forces Command analysis of cyber-related joint doctrine. To assess the extent to which DOD has assigned command and control responsibilities, we compared the 2008 Unified Command Plan to DOD plans, policies, and guidance to determine authorities for functional and combatant commands, military services, and defense agencies. Additionally, we reviewed and identified common lessons learned from combatant commands following DOD's response to malware infections in 2008. To determine any capability gaps involving computer network operations we analyzed the fiscal year 2010 and 2011-2015 Integrated Priority Lists to identify cyberspace capability gaps for the functional and geographic combatant commands.⁶ Finally, we analyzed the National Intelligence Estimate, *The Global Cyber Threat to the U.S. Information Infrastructure*, the Central Intelligence Agency's *Cyber Threat Intelligence Highlights*, and prior GAO reports on cybersecurity to determine the depth of cyber threats facing the nation and DOD.

We conducted this performance audit from November 2008 to April 2010 in accordance with generally accepted government auditing standards and worked with DOD from November 2010 to July 2011 to prepare an unclassified version of this report for public release. Government auditing standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Results in Brief

DOD's organization to address cybersecurity threats is decentralized and spread across various offices within the Office of the Secretary of Defense, the Joint Staff, functional and geographic combatant commands, military services, and military agencies. Cybersecurity roles

⁶An Integrated Priority List is a list of a combatant commander's highest priority requirements, prioritized across service and functional lines, defining shortfalls in key programs that, in the judgment of the combatant commander, adversely affect the capability of the combatant commander's forces to accomplish their assigned mission. The integrated priority list provides the combatant commander's recommendations for programming funds in the planning, programming, and budgeting system process.

and responsibilities for DOD are vast and include developing joint policy and guidance and operational functions to protect and defend DOD's computer networks. These responsibilities are spread throughout DOD. For example, joint policy development responsibilities reside in several offices in the Office of the Secretary of Defense and the Joint Staff, and operational responsibilities reside in the U.S. Strategic Command, the Defense Information Systems Agency, the military services, and the combatant commands. Other organizations play key roles in cybersecurity; these include the DOD intelligence agencies that provide intelligence in support of computer network operations, the National Guard units that augment DOD's cyber force, and defense criminal investigative organizations that conduct cyber-related criminal and counterintelligence investigations. DOD is now taking proactive measures to better address cybersecurity threats, such as addressing what it recognizes as a lack of integration of computer network operations at the command and operational levels. DOD is developing new organizational structures to facilitate the integration of cyber operations. These efforts include (1) establishing the U.S. Cyber Command, at the direction of the Secretary of Defense in June 2009, to lead, organize, and integrate military cyber operations; (2) restructuring the Office of the Under Secretary of Defense for Policy to establish a lead focal point for cyber policy; and (3) establishing new organizations within the military services to support the U.S. Cyber Command. These are important initiatives to help centralize cyber policy and direction. However, it is too early to tell if these ongoing organizational changes will improve DOD's overall cyber efforts and allow it to better address cybersecurity threats.

Several joint doctrine publications address aspects of cyberspace operations, but DOD officials acknowledge that the discussions are insufficient, and no single joint publication completely addresses cyberspace operations. According to DOD, the purpose of joint doctrine is to enhance the operational effectiveness of U.S. forces, and it should consist of fundamental principles that guide the employment of U.S. military forces in coordinated action toward a common objective—including terms, tactics, techniques, and procedures.⁷ While DOD assesses that at least 16 DOD joint publications discuss cyberspace-related topics and 8 mention "cyberspace operations," U.S. Joint Forces

⁷Chairman, Joint Chiefs of Staff, Instruction 5120.02B, *Joint Doctrine Development System* (Washington, D.C., Dec. 4, 2009).

Command has concluded that none contained a sufficient discussion of cyberspace operations. For instance, according to U.S. Strategic Command, the publication with the majority of cyberspace-related references, Joint Publication 3-13, *Information Operations*,⁸ was sufficient when written several years ago but it has become insufficient for current cyber operations and omits important elements of the definition of computer network operations. Other definitions—such as what constitutes a cyber force—are not uniformly defined across DOD, and there are cases in which the same cyber-related term may mean something different among the services. A joint publication focusing on all aspects of cyberspace operations is expected to enhance the operational effectiveness of force development, as cyberspace is inherently joint and cuts across all combatant commands, services, and agency boundaries. DOD recognizes the need to develop and update cyber-related joint doctrine and is currently debating the merits of developing a single cyberspace operations joint doctrine publication in addition to updating all existing doctrine with respect to cyberspace operations. However, it has not established time frames for the completion of either of these efforts. We are recommending that DOD establish a time frame for (1) deciding to proceed with a dedicated joint doctrine publication on cyberspace operations and for (2) updating the existing body of joint doctrine to include complete cyberspace-related definitions.

DOD has assigned authorities and responsibilities for implementing cyber operations among combatant commands and military services; however, the supporting relationships necessary to achieve command and control of cyber operations remain unclear. According to the *National Military Strategy for Cyberspace Operations*, the United States can achieve superiority in cyberspace only if command and control relationships are clearly defined and executed.⁹ It further states that these

⁸Chairman, Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations* (Washington, D.C., Feb. 13, 2006). This publication is currently being revised by DOD.

⁹According to DOD, the *National Military Strategy for Cyberspace Operations* is the department's strategy to assure U.S. military superiority in cyberspace. The strategy establishes a common understanding of cyberspace and sets forth a military strategic framework that orients and focuses DOD action in the areas of military, intelligence, and business operations in and through cyberspace. Combatant commands, military departments, agencies, field activities, and other DOD organizational entities should use the strategy as a definitive reference to plan, execute, and resource cyberspace operations.

relationships must support unity of effort in achieving combatant commander missions as well as maintaining freedom of action in cyberspace. The 2008 Unified Command Plan assigns to the commander of U.S. Strategic Command specific responsibilities that include directing global information grid operations and defense, planning against cyberspace threats, coordinating with other combatant commands and U.S. government agencies, integrating support activities, and executing cyberspace operations as directed. But the 2008 Unified Command Plan also states that geographic combatant commanders are to exercise authority over all commands and forces within their areas of responsibility, which has led to confusion among the combatant commands about command and control for cyber operations.¹⁰ Under the current DOD Standing Rules of Engagement, unit commanders always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstrated hostile intent, but additional procedures for coordination and approval apply for cyber operations. Additionally, individual service components that operate networks residing in a geographic combatant command currently report to their respective service organizations and not to the geographic combatant commander. This affects the geographic combatant commanders' visibility over networks that reside in their areas of responsibility. For example, after a malware eradication effort was undertaken by DOD in 2008, U.S. Strategic Command identified confusion regarding command and control authorities and chains of command because the exploited network fell under the purview of both U.S. Strategic Command, military services, and a geographic combatant command.¹¹ This led to uncoordinated, conflicting, and unsynchronized guidance in response to the incident being issued in several forms via multiple channels from both U.S. Strategic Command and Joint Task Force–Global Network Operations. Our review confirmed that multiple directives contributed to confusion at

¹⁰Geographic combatant commanders are responsible for specific air, land, and sea areas of responsibility throughout the world. Examples include Pacific Command and Central Command. Functional combatant commands are responsible for specific types of operational support to the geographic commands, such as Transportation Command for air, land, and sea transport and Strategic Command for strategic nuclear, space, and other operations—such as cyberspace.

¹¹Malware is defined as software designed to carry out annoying or harmful actions. Malware often masquerades as a useful program or is embedded into useful programs, so that users are induced into activating it. Malware can also be installed without the user's knowledge to surreptitiously track or transmit data, or both, to an unauthorized third party.

the execution level, leaving operators and administrators to reconcile priorities and question which procedures were appropriate and most urgent to address the malware infection. Although DOD intends for the new U.S. Cyber Command to facilitate command and control, as late as December 2009, DOD noted that these problems had not been addressed, though the new U.S. Cyber Command is expected to be established by October 2010. Without complete and clearly articulated guidance on command and control responsibilities that is well-communicated and practiced with key stakeholders, DOD will have difficulty in achieving command and control of its cyber forces globally and in building unity of effort for carrying out cyber operations. Therefore, we are recommending that DOD clarify its guidance on command and control relationships between U.S. Strategic Command, the services, and the geographic combatant commands regarding cyberspace operations.

DOD has identified some cyberspace capability gaps, but it has not completed a comprehensive, departmentwide assessment of needed resources, capability gaps, and an implementation plan for addressing any gaps. A broad range of DOD strategy, operational concepts, and studies highlights the importance of developing the appropriate capabilities necessary to conduct cyberspace operations, including trained personnel, infrastructure, and organizational structures. Further, DOD's structure for defining and developing key capabilities for joint operations includes a framework for conducting comprehensive assessments of capability needs and gaps so that solutions can be found to address them. DOD has gathered information on some cyberspace gaps reported by the combatant commands through integrated priority lists. For example, U.S. Strategic Command, which is tasked with executing both computer network defense and computer network attack in support of combatant commands, noted that DOD's cyber workforce is insufficient to meet its current needs, which are projected to increase significantly over time. Other combatant commands reported insufficient numbers of trained personnel to support their cyber operations and a need for additional cyber capabilities. In June 2009, the Joint Staff reviewed and endorsed 85 capability gaps resulting from the integrated priority lists, including 4 cyber-related gaps.¹² Furthermore, the Joint Staff

¹²DOD, *Fiscal Year 2011-2015 Capability Gap Assessment Results and Recommendations for Mitigating Capability Gaps*, JROCM 113-09 (Washington D.C., June 2009).

stated that the Functional Capabilities Boards¹³ will track proposed actions—such as cyber manpower—to address these capability gaps. While DOD’s review of the reported cyberspace capability gaps and various studies on cyberspace operations are steps in the right direction, it remains unclear whether these gaps will be addressed since DOD has not conducted a comprehensive departmentwide assessment of cyber-related capability gaps or established an implementation plan or specific time frames to resolve any gaps that may be identified. In addition to the Joint Staff’s ongoing efforts to track the fiscal years 2011-2015 capability gaps, and because of the increased importance associated with the DOD’s cyber domain, we recommend that DOD conduct a comprehensive departmentwide cyberspace capabilities-based assessment and develop an implementation plan and funding strategy to address any resulting identified gaps.

DOD provided written comments on a draft of this report. DOD concurred with our recommendations and discussed some of the steps it is taking and planning to take to address these recommendations. DOD also provided technical comments, which we have incorporated into the report where appropriate. DOD’s response is reprinted in appendix V.

Background

National Cyber Policy

As cyber threats have grown in sophistication, federal efforts to address them have evolved. Presidential Decision Directive 63, signed in May 1998, established a structure under White House leadership to coordinate the activities of designated lead departments and agencies, in partnership with their counterparts from the private sector, to eliminate any significant vulnerabilities to both physical and cyber attacks on our critical

¹³Functional Capabilities Boards are created by the Joint Requirements Oversight Council and are responsible for the organization, analysis, and prioritization of joint warfighting capabilities within an assigned functional area. There are multiple functional capability boards assigned with tracking and reporting on the fiscal years 2011-2015 capability gaps. The Battlespace Awareness Functional Capabilities Board and the Force Support Functional Capabilities Board have been tasked with tracking 3 of the 4 cyber-related capability gaps. While the Joint Staff has directed the Functional Capabilities Boards to track the recommendations and report back to the Joint Requirements Oversight Council, they can only act as an adviser to the council.

infrastructures, including computer systems.¹⁴ National cyber policy was updated in 2003 with *The National Strategy to Secure Cyberspace*.¹⁵ Presidential Decision Directive 63 was superseded later that year by Homeland Security Presidential Directive 7, which assigned the Secretary of Homeland Security responsibility for coordinating the nation's overall critical infrastructure protection efforts, including protection of the cyber infrastructure, across all sectors (federal, state, local, and private) working in cooperation with designated sector-specific agencies within the executive branch.¹⁶ Both of these policies focused on defensive strategies, and Homeland Security Presidential Directive 7 did not emphasize protection of federal government information systems. Subsequent classified presidential directives and strategic planning documents have continued to reflect evolving federal policy in response to cyber threats.

Recognizing the need for common solutions to improve cybersecurity, the White House, Office of Management and Budget, and various federal agencies have launched or continued several governmentwide initiatives that are intended to enhance information security at federal agencies. According to Director of National Intelligence implementing guidance, in 2008 the Comprehensive National Cybersecurity Initiative was begun in order to develop an approach to address current threats, anticipate future threats and technologies, and foster innovative public-private partnerships.¹⁷ It was created to bridge cyber-related missions for federal agencies, by asking them to undertake a set of 12 initiatives and 7 strategic enabling activities.¹⁸ According to DOD officials, these initiatives

¹⁴The White House, Presidential Decision Directive 63, *Critical Infrastructure Protection* (May 22, 1998).

¹⁵Office of the White House, *The National Strategy to Secure Cyberspace* (Washington, D.C., February 2003).

¹⁶The White House, Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection* (Dec. 17, 2003).

¹⁷President George W. Bush approved the plan on January 8, 2008. The White House, National Security Presidential Directive 54 / Homeland Security Presidential Directive 23, *Cybersecurity Policy* (Jan. 8, 2008).

¹⁸DOD participates in the following initiatives: (1) deployment of intrusion prevention system; (2) increase the security of the classified networks; (3) expand education; (4) develop multi-pronged approach for global supply chain risk management. It is also involved in 2 enablers involving increasing DOD information assurance and predictive behavioral information and trend analysis.

include defensive, offensive, research and development, and counterintelligence efforts. Programs focus primarily on the security of executive-branch networks, which represent only a fraction of the global information and communications infrastructure on which the United States depends.

In May 2009, the National Security Council and Homeland Security Council completed a 60-day interagency review intended to assess U.S. policies and structures for cybersecurity and outline initial areas for action.¹⁹ The resulting report recommended, among other things, appointing an official in the White House to coordinate the nation's cybersecurity policies and activities, preparing an updated national cybersecurity strategy, developing a framework for cyber research and development, and continuing to evaluate the Comprehensive National Cybersecurity Initiatives.

DOD Policy Guidance on Cybersecurity

Following the lead of federal government efforts, DOD initiated several efforts to develop policy and guidance on cyberspace operations. In 2006 and 2007, *The National Military Strategy for Cyberspace Operations* and associated *Implementation Plan* provided a strategy for the U.S. military to achieve military superiority in cyberspace and established a military strategic framework that orients and focuses DOD action in the areas of military, intelligence, and business operation in and through cyberspace.²⁰ In 2008, U.S. Strategic Command developed the *Operational Concept for Cyberspace*, which identifies near-term concepts to improve operations in and through cyberspace and gain superiority over potential adversaries in support of national objectives.²¹ The 2009 *Quadrennial Roles and Missions Review Report* discussed efforts by the Cyber Issue Team, jointly led by the Office of the Under Secretary of Defense for Policy and U.S. Strategic Command, which addressed cyberspace issues related to

¹⁹The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C., May 29, 2009).

²⁰DOD, *The National Military Strategy for Cyberspace Operations* (Washington, D.C., December 2006) and DOD, *The National Military Strategy for Cyberspace Operations Implementation Plan* (Washington, D.C., September 2007).

²¹DOD, *Operational Concept for Cyberspace* (Offutt Air Force Base, Neb., April 2008).

developing, structuring, and employing the cyberspace force.²² Also in 2009, U.S. Strategic Command developed an Operations Order titled Operation Gladiator Phoenix to provide DOD with a strategic framework to operate, secure, and defend the global information grid. As early as 2006, the Quadrennial Defense Review highlighted the department's need to be capable of shaping and defending cyberspace. DOD published a new Quadrennial Defense Review in February 2010, which designated cyberspace operations as a key mission area and discussed steps the department was taking to strengthen capabilities in the cyber domain, including centralizing command of cyber operations and enhancing partnerships with other agencies and governments. Currently, DOD continues to develop and update cyberspace policies.

Cybersecurity Threats

Different types of cybersecurity threats from numerous sources may adversely affect computers, software, networks, agency operations, industry, or the Internet itself. Cyber threats to federal information systems continue to evolve and grow. These threats can be unintentional or intentional, targeted or nontargeted, and can come from a variety of sources. Unintentional threats can be caused by inattentive or untrained employees, software upgrades, maintenance procedures, and equipment failures that inadvertently disrupt systems or corrupt data. Intentional threats include both targeted and nontargeted attacks. An attack is considered to be targeted when a group or individual attacks a specific system or cyber-based critical infrastructure. A nontargeted attack occurs when the intended target of the attack is uncertain, such as when a virus, worm, or other malicious software is released on the Internet with no specific target.

Government officials are concerned about cyber attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. Threats to DOD computer networks posed by the intelligence branches of foreign countries and hackers alike represent an unprecedented national security challenge. For example, in February 2009, the Director of National Intelligence testified that foreign nations and criminals have targeted government and private-sector networks to gain a competitive advantage and potentially disrupt or destroy them, and

²²DOD, *Quadrennial Roles and Missions Review Report* (Washington, D.C., January 2009).

that terrorist groups have expressed a desire to use cyber attacks as a means to target the United States.²³ The Federal Bureau of Investigation has also identified multiple sources of threats to our nation's critical information systems, including foreign nations engaged in espionage and information warfare, domestic criminals, hackers, virus writers, and disgruntled employees and contractors working within an organization. Table 1 summarizes those groups or individuals that are considered to be key sources of cyber threats to our nation's information systems and cyber infrastructures.

Table 1: Sources of Cyber Threats

Threat source	Description
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. According to the Director of National Intelligence, ^a a growing array of state and nonstate adversaries are increasingly targeting—for exploitation and potential disruption or destruction—information infrastructure, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
Criminal groups	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Insiders	Working from within an organization, the insider threat can be intentional or unintentional. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat remains one of the most significant cyber threats to DOD. The insider threat can also include contractor personnel.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries.

Source: GAO and GAO analysis of Office of Director of National Intelligence information.

^aPrepared statement of Dennis Blair, Director of National Intelligence, before the Senate Select Committee on Intelligence, Feb. 12, 2009.

²³Prepared Statement of Dennis Blair, Director of National Intelligence, before the Senate Select Committee on Intelligence, Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence (Feb. 12, 2009).

These groups and individuals have a variety of attack techniques at their disposal. Furthermore, as we have previously reported, the techniques have characteristics that can vastly enhance the reach and effect of their actions, such as the following:

- Attackers do not need to be physically close to their targets to perpetrate a cyber attack.
- Technology allows actions to easily cross multiple state and national borders.
- Attacks can be carried out automatically, at high speed, and by attacking a vast number of victims at the same time.
- Attackers can more easily remain anonymous.²⁴

Table 2 identifies the types and techniques of cyber attacks that are commonly used.

Table 2: Types and Techniques of Cyber Attacks

Threat source	Description
Botnet	A network of remotely controlled systems used to coordinate attacks and distribute malware, spam, and phishing scams. Bots (short for “robots”) are programs that are covertly installed on a targeted system allowing an unauthorized user to remotely control the compromised computer for a variety of malicious purposes.
Denial of service	A method of attack that denies system access to legitimate users without actually having to compromise the targeted system. From a single source, the attack overwhelms the target computers with messages and blocks legitimate traffic. It can prevent one system from being able to exchange data with other systems or prevent the system from using the Internet.
Distributed denial of service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bomb	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer’s employment.
Malware	Malicious software designed to carry out annoying or harmful actions. Malware often masquerades as a useful program or is embedded into useful programs, so that users are induced into activating programs. Can also be installed without the user’s knowledge to surreptitiously track or transmit data, or both, to an unauthorized third party.

²⁴GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, [GAO-07-705](#) (Washington, D.C.: June 22, 2007).

Threat source	Description
Pharming	A method used by phishers to deceive users into believing that they are communicating with a legitimate Web site. Pharming uses a variety of technical methods to redirect a user to a fraudulent or spoofed Web site when the user types a legitimate Web address.
Phishing	A high-tech scam that frequently uses spam or pop-up messages to deceive people into disclosing sensitive information. Internet scammers use e-mail bait to “phish” for passwords and financial information from the sea of Internet users.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Spamming	Sending unsolicited commercial e-mail advertising for products, services, and Web sites. Spam can also be used as a delivery mechanism for malicious software and other cyber threats.
Spoofing	Creating a fraudulent Web site to mimic an actual, well-known site run by another party. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message.
Trojan horse	A computer program that conceals harmful code. A trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that “infects” computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected files are loaded into memory, allowing the virus to infect other files. Unlike the computer worms, a virus requires human involvement (usually unwitting) to propagate.
War-dialing	Using a simple program to dial consecutive phone numbers looking for a modem.
War-driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

Source: GAO.

Key Terms for DOD’s Cyberspace Domain

Various terms are used within the DOD cyberspace domain. For example, in May 2008, DOD defined cyberspace as the “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”²⁵ Also, DOD defines computer network defense as actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. For further discussion of policies, programs, and

²⁵Memorandum from the Deputy Secretary of Defense, *The Definition of Cyberspace* (May 12, 2008). This definition was adopted for consistency with the recently promulgated National Security Presidential Directive 54 / Homeland Security Presidential Directive 23.

tools that DOD uses to protect its networks, see appendix III. Table 3 lists several key terms used within the DOD cyberspace domain.

Table 3: Key Terms for DOD Cyberspace

Term	Description
Computer network attack	Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
Computer network attack operational preparation of the environment	Operations conducted to gain or confirm access to, or both, and gather key information on the target network concerning the capabilities and configuration of targeted networks or systems and to facilitate target acquisition and target analysis in preparation for computer network attack or other offensive missions. These activities facilitate subsequent computer network attack or other offensive missions by identifying a window of opportunity when computer network attack or other offensive missions will be most likely to succeed. The authority to conduct computer network attack operational preparation of the environment is inherent in the authority to conduct computer network attack. This activity does not include the intentional acquisition of communications information for the purpose of foreign intelligence.
Computer network defense	Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. The unauthorized activity may include disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems or their contents, or theft of information. As a part of computer network defense it includes information assurance protection activity and includes deliberate actions taken to modify an assurance configuration or condition in response to a computer network defense alert or threat information.
Computer network defense response actions	Deliberate, authorized defensive measures or activities that protect and defend DOD computer systems and networks under attack or targeted for attack by adversary computers systems/networks.
Computer network exploitation	Enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks.
Computer network operations	Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.
Cyberspace operations	The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the global information grid.
Global information grid	The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel. It also includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority.
Information assurance	Measures taken to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
Information operations	The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own.

Term	Description
JWICS	The Joint Worldwide Intelligence Communications System (JWICS), owned and operated by the Defense Intelligence Agency, is the Top Secret/Sensitive Compartmented Information component of the Defense Information Services Network that connects members of the Department of Defense intelligence information systems community, non-Department of Defense intelligence information systems community, and the intelligence community.
Network operations	Commonly referred to as NetOps, this is the DOD-wide operational, organizational, and technical capabilities for operating and defending the global information grid.
NIPRNet	The unclassified but sensitive Non-classified Internet Protocol Router Network to support unclassified Internet protocol data communications services for combat support applications to the Department of Defense, Joint Chiefs of Staff, military departments, and combatant commands.
SIPRNet	The secret Internet protocol router network is DOD's largest interoperable command and control data network, supporting the global command and control system, the defense message system, collaborative planning, and numerous other classified warfighter applications.

Source: GAO compilation from various DOD sources.

Cybersecurity Roles and Responsibilities Are Spread across DOD, and DOD Is Reorganizing to Better Address Cybersecurity Threats

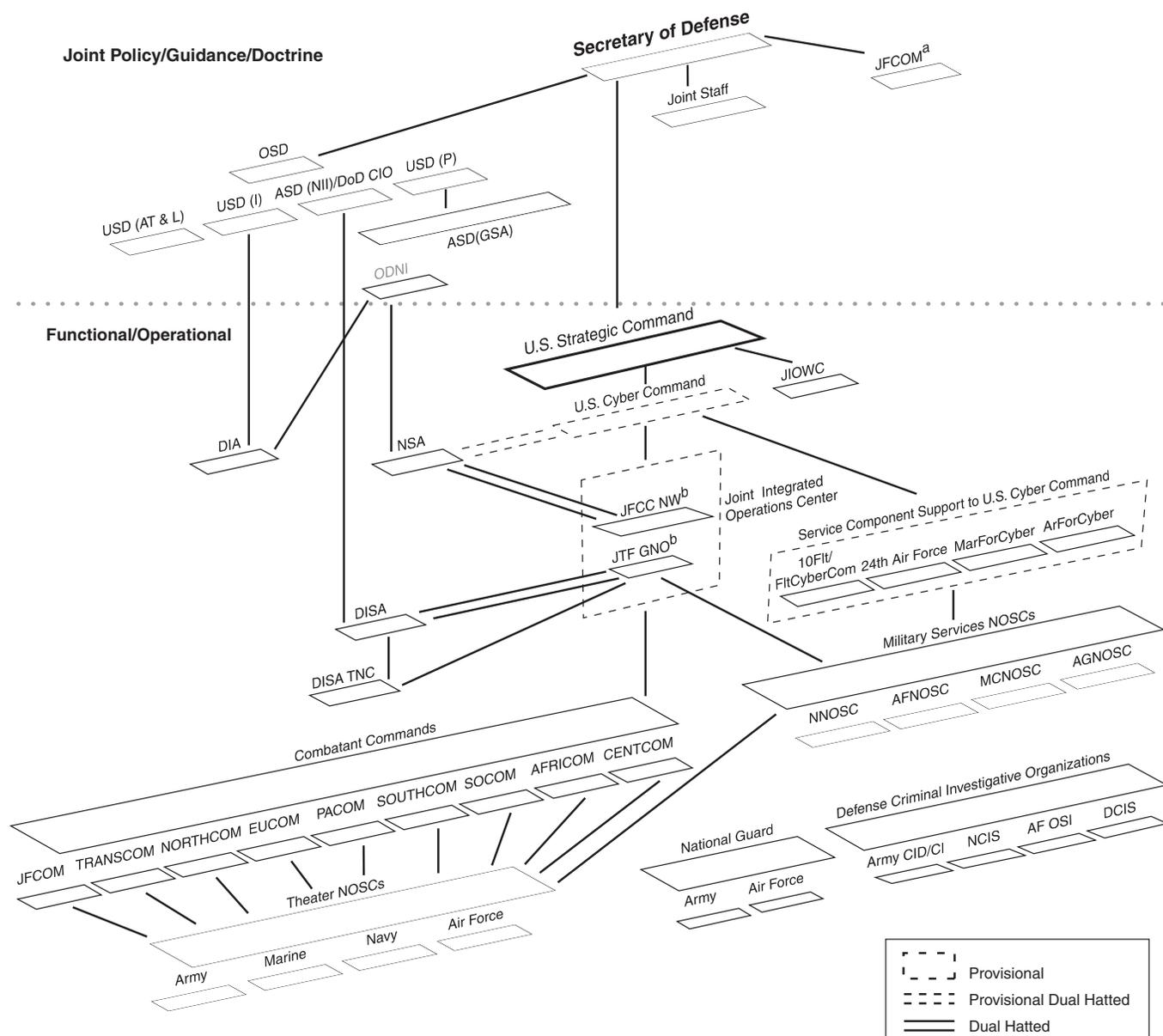
DOD's organization to address cybersecurity threats is decentralized and spread across various offices, commands, military services, and military agencies. DOD cybersecurity roles and responsibilities are vast and include developing joint policy and guidance and operational functions to protect and defend its computer networks. DOD is taking proactive measures to better address cybersecurity threats, such as developing new organizational structures, led by the establishment of the U.S. Cyber Command, to facilitate the integration of cyberspace operations.

Cybersecurity Roles and Responsibilities Are Spread across DOD

Cybersecurity roles and responsibilities within DOD are spread across various DOD components. The current cybersecurity organizational structure is decentralized and there are many DOD components that hold responsibilities. Cybersecurity roles and responsibilities include developing joint policy and guidance and operational functions to defend and secure DOD networks, and are spread among the Office of the Secretary of Defense, Joint Staff, functional and geographic combatant commands, military services, and military agencies. According to DOD officials, to ensure a holistic approach and limit potential stovepiping, the department has begun to develop cybersecurity expertise across various offices. Figure 1 illustrates DOD's cyber organization as of March 2010. Additionally, there are other organizations that play a pivotal role in cybersecurity, such as the DOD intelligence agencies, National Guard, and defense criminal investigative organizations. DOD is taking proactive measures to reorganize and develop new organizational structures to better address cybersecurity threats. However, it is too early to tell if

these organizational changes will help DOD better address cybersecurity threats.

Figure 1: DOD Cyber Organization as of March 2010



Source: GAO analysis of DoD information.

Legend:

10th Fleet: Navy Fleet Forces Cyber Command

JIOWC: Joint Information Operations Warfare Center

Legend:

24th Air Force

AF OSI: Air Force Office of Special Investigations

AFNOSC: Air Force Network Operations Security Center

AFRICOM: U.S. Africa Command

AGNOSC: Army Global Network Operations Security Center

ArForCyber: Army Forces Cyber

Army CI / CID: Army Counter Intelligence and Army Criminal Investigative Command

ASD(GSA): Assistant Secretary of Defense for Global Strategic Affairs

ASD(NII) / DOD CIO: Assistant Secretary of Defense, Network Information and Integration / DOD Chief Information Officer

CENTCOM: U.S. Central Command

CIG: Computer Information Group

CIT: Computer Information Team

COCOM: U.S. Combatant Command

DCIS: Defense Criminal Investigative Services

DIA: Defense Intelligence Agency

DISA: Defense Information Systems Agency

EUCOM: U.S. European Command

JFCC NW: Joint Functional Component Command for Network Warfare

JFCOM: U.S. Joint Forces Command

JTF GNO: Joint Task Force—Global Network Operations

MarForCyber: Marine Forces Cyber

MCNOSC: Marine Corps Network Operations Security Center

NCIS: Naval Criminal Investigative Service

NNOSC: Navy Network Operations Security Center

NORTHCOM: U.S. Northern Command

NOSC: Network Operations Security Center

NSA: National Security Agency

ODNI: Office of the Director of National Intelligence

OSD: Office of Secretary of Defense

PACOM: U.S. Pacific Command

SOCOM: U.S. Special Operations Command

SOUTHCOM: U.S. Southern Command

TNC: Theater Network Operations Center

^aAccording to Joint Publication 1.0, U.S. Joint Forces Command is responsible for recommending changes in doctrine.

^bAccording to DOD, Joint Functional Component Command for Network Warfare and Joint Task Force—Global Network Operations will be disestablished by full operational standup of the U.S. Cyber Command.

Numerous DOD Organizations Are Responsible for Developing Cyber Joint Policy, Guidance, and Doctrine

There are several offices within both the Office of the Secretary of Defense and the Joint Staff that share responsibility for developing joint cyber policy, guidance, and doctrine for DOD activities that occur in and through cyberspace. For example, within the Office of the Secretary of Defense, the offices of the Under Secretary of Defense for Policy; Assistant Secretary of Defense for Networks and Information Integration; and the Under Secretary of Defense for Intelligence, all share responsibility for developing joint cyber policy and guidance. For example, according to DOD officials, both the Assistant Secretary of Defense for Networks and Information Integration and the Under Secretary of Defense for Policy have responsibility for strategic-level guidance and oversight for computer network operations and information assurance. Appendix II

provides more detailed information on the cyber-related responsibilities of the DOD offices.

Several offices within the Joint Staff also hold responsibilities for developing joint cyber policy, guidance, and doctrine for DOD activities that occur in and through cyberspace. The Joint Staff's cyber responsibilities include establishing and developing doctrine, policies, and associated joint tactics, techniques, and procedures for DOD's global information grid, information assurance, and joint and combined operations. According to DOD directive O-3600.01, the Joint Staff is to develop and maintain joint doctrine for core, supporting, and related information operations capabilities in joint operations and ensure that all joint education, training, plans, and operations are consistent with information operations policy, strategy, and doctrine.²⁶ The Joint Staff is also responsible for developing, coordinating, and disseminating information assurance policies and doctrine for joint operations. Additionally, several Joint Staff divisions and Joint Staff-led coordination forums have cybersecurity responsibilities.

The U.S. Joint Forces Command also has doctrine development and operational roles. Chairman of the Joint Chiefs of Staff Instruction 5120.02B establishes U.S. Joint Forces Command as a voting member of the joint doctrine development community, responsible for developing and submitting recommendations for improving existing joint doctrine or initiating new joint doctrine projects and conducting front-end analyses of all joint doctrine project proposals and providing appropriate recommendations.²⁷ Moreover, as with all other combatant commands, U.S. Joint Forces Command is responsible for conducting computer network defense to secure its portion of the DOD global information grid, including developing and implementing information operations and information assurance programs and activities.

²⁶U.S. Department of Defense, Directive O-3600.01, *Information Operations* (Washington, D.C., Aug. 14, 2006).

²⁷Chairman, Joint Chiefs of Staff, Instruction 5120.02B, *Joint Doctrine Development System*.

Numerous DOD Organizations Have Operational Responsibilities to Defend and Secure DOD Computer Networks

DOD also has numerous organizations with operational roles and responsibilities to defend and secure DOD computer networks. U.S. Strategic Command is considered the lead for cyberspace operations within DOD. According to the 2008 Unified Command Plan, U.S. Strategic Command is responsible for synchronizing DOD's planning for cyberspace operations, and it does so in coordination with other combatant commands, the military services, and defense agencies.²⁸

In order to operationalize its missions, U.S. Strategic Command delegated operational and tactical-level planning, force execution, and day-to-day management of forces to its joint functional component commands. Prior to the establishment of U.S. Cyber Command, these component commands conducted cyberspace-related operations for the U.S. Strategic Command while headquarters focuses on strategic-level integration and advocacy. These component commands were as follows:

- Joint Functional Component Command for Network Warfare (JFCC NW), which was responsible for planning, integrating, and coordinating cyberspace capabilities and integrating with all necessary computer network operations capabilities.
- Joint Task Force–Global Network Operations, which was responsible for DOD's global network operations and directing the operation and defense of DOD's global information grid.
- Joint Information Operations Warfare Center, which is the lead entity responsible for planning, integrating, synchronizing, and advocating for information operations across DOD including computer network operations, electronic warfare, psychological operations, military deception, and operations security.

In June 2009, as part of the creation of U.S. Cyber Command, U.S. Strategic Command was directed by the Secretary of Defense to disestablish Joint Task Force–Global Network Operations and Joint Functional Component Command for Network Warfare in preparation for U.S. Cyber Command reaching its full operating capability, planned for October 2010. Additionally, the military departments were directed to identify and provide appropriate component support to U.S. Cyber Command to be in place and functioning by that same date.

²⁸DOD, *Unified Command Plan* (Washington, D.C., Dec. 17, 2008).

Other combatant commands also have operational roles and responsibilities for defending and securing DOD computer networks. According to DOD Directive 8500.01E, the combatant commands must also develop and implement their own information assurance programs for their respective portions of the DOD global information grid and must provide training and education for their information assurance personnel.²⁹ Certain combatant commands have unique responsibilities. For instance, U.S. Northern Command has specific responsibilities and is the DOD lead in assisting the Department of Homeland Security and other civilian agencies during cyber-related incidents as part of its Defense Support of Civil Authorities missions—or civil support. During these incidents, U.S. Northern Command—and in some instances U.S. Pacific Command—will be supported by U.S. Strategic Command. Functional combatant commands have a global mission and a global requirement for network operations support. Some functional combatant commands, such as U.S. Special Operations Command, operate their own specific functional global networks.

The military service components have a significant role in providing cybersecurity while operating and defending their respective networks within DOD's global information grid. In their role, each military service is responsible for fielding, training, and equipping cyberspace forces. They also protect, defend, and conduct restoration measures for the networks they control, and ensure that service-managed portions of DOD's global information grid are secure and interoperable, with appropriate information assurance and trained personnel. Appendix II has more information on the military services' current cyber organization.

Defense agencies also share responsibilities related to cyber operations. For example, the Defense Information Systems Agency is a combat support agency responsible for the day-to-day management of DOD's global information grid, communication and computer-based information systems, and performs significant network operations support functions. Together with the military services, the agency has the responsibility to build, maintain, and operate DOD's global information grid. It is also responsible for employing information assurance operations and securing DOD's enterprise systems. The agency reports to the Assistant Secretary

²⁹DOD, Directive 8500.01E, *Information Assurance (IA)* (Washington, D.C., Oct. 24, 2002) (certified current as of Apr. 23, 2007).

of Defense for Network and Information Integration, and its director also currently commands Joint Task Force–Global Network Operations.

There are many other agencies and organizations that support DOD cyber efforts, including the DOD intelligence agencies, the National Guard, and defense criminal investigative organizations. The intelligence agencies play an integral role in enhancing cybersecurity both by increasing our ability to detect and identify adversary cyber activity and by expanding our knowledge of the capabilities, intentions, and cyber vulnerabilities of our adversaries. For example, the National Security Agency provides information assurance support to DOD, prescribes minimum standards for protecting national security systems, and provides warning support to other DOD components. The Director of the National Security Agency was also designated to serve as commander of the Joint Functional Component Command for Network Warfare.³⁰ The Defense Intelligence Agency is a combat support agency that provides all-source intelligence to combatant commanders, defense planners, and national security policymakers, as well as manages, operates, and maintains its own network and information assurance program. The Office of the Director for National Intelligence provides direction for signals intelligence collection in cyberspace through the National Intelligence Strategy and National Intelligence Priority Framework. The National Guard—comprising the Army National Guard and Air National Guard—provides cyber capabilities to meet military service and combatant commander requirements and can be leveraged under state authorities to assist civil authorities. According to Air National Guard officials, skilled personnel that come from information technology, banking, and other sectors have been utilized to provide cyber capabilities to agencies with insufficient manpower.

Defense criminal investigative organizations conduct cyber-related criminal and counterintelligence investigations that may involve offenses

³⁰In June 2009, as part of the creation of U.S. Cyber Command, U.S. Strategic Command was directed by the Secretary of Defense to disestablish Joint Task Force–Global Network Operations and Joint Functional Component Command for Network Warfare in preparation for U.S. Cyber Command reaching its full operating capability, planned for October 2010. Additionally, the military departments were directed to identify and provide appropriate component support to U.S. Cyber Command to be in place and functioning by that same date. .

under title 18 of the U.S. Code.³¹ These organizations include: (1) the Naval Criminal Investigative Service; (2) the Air Force Office of Special Investigations; (3) the Defense Criminal Investigative Service; (4) the Army Criminal Investigation Command; (5) Army Counterintelligence, and the related DOD Cyber Crime Center.

DOD Is Reorganizing to Better Address Cybersecurity Threats

DOD is taking proactive measures to reorganize and develop new organizational structures to better address cybersecurity threats. As a result of significant cyber challenges and organizational constraints, DOD is conducting a multitiered organizational restructuring for cyber organizations, including the establishment of the U.S. Cyber Command, and changes within the Office of the Secretary of Defense and the military services.

U.S. Cyber Command

The establishment of U.S. Cyber Command is DOD's primary organizational change to better address cybersecurity threats. On June 23, 2009, the Secretary of Defense signed a memorandum directing U.S. Strategic Command to establish the U.S. Cyber Command as a subordinate unified command with responsibility for military cyberspace operations.³² In this memorandum, the Secretary of Defense stressed the new national security risks that arise from DOD's increasing dependency on cyberspace and the growing array of cyber threats and vulnerabilities. DOD has recognized that it lacks integration of computer network operations at the command and operational levels. DOD anticipates that the U.S. Cyber Command will focus on the integration of cyberspace operations, will synchronize DOD cyber missions and warfighting efforts, and will provide support to civil authorities and international partners.

The Secretary of Defense recommended that the director of the National Security Agency become the commander of the U.S. Cyber Command and that the command retain current authorities to conduct cyberspace responsibilities that had been given to the U.S. Strategic Command in the 2008 Unified Command Plan. Additionally, U.S. Strategic Command will delegate its cyberspace missions to U.S. Cyber Command in a phased

³¹GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, [GAO-07-705](#) (Washington, D.C.: June 22, 2007).

³²Secretary of Defense, *Memorandum Establishing the U.S. Cyber Command* (Washington D.C., June 2009).

approach. Initial operating capability was established in October 2009; and full operational capability is anticipated in October 2010. By full operational capability, U.S. Strategic Command will disestablish both the Joint Task Force–Global Network Operations and the Joint Functional Component Command for Network Warfare, and their existing personnel will be incorporated into the new subunified command. As a result, the Director of the Defense Information Systems Agency will relinquish all duties as the Commander of the Joint Task Force–Global Network Operations. However, the Defense Information Systems Agency will establish a field office and a support element at U.S. Cyber Command to ensure an operational linkage between the new command and the agency.

The Secretary of Defense also directed actions in his own office and in each military service intended to improve the diffuse efforts related to cyberspace operations. In response, the Office of the Under Secretary of Defense for Policy is leading a review of policy and strategy to develop a comprehensive approach to DOD cyberspace operations. Additionally, the Office of the Under Secretary of Defense for Policy is conducting an organizational realignment to better address cybersecurity. The office created a separate division—Deputy Assistant Secretary of Defense for Cyber and Space Policy—to be a central focal point for cyberspace policy in the Office of the Secretary of Defense. The military services are also working to identify and provide appropriate component support to the U.S. Cyber Command prior to its full operational capability in October 2010. The military services are developing and implementing the following new initiatives. On January 29, 2010, the U.S. Navy established the Fleet Cyber Command, 10th Fleet to provide component support to the U.S. Cyber Command. The Air Force initially planned to establish a major cyber command. Instead, it stood up the 24th Air Force which will provide cyber forces and capabilities to the U.S. Cyber Command. The Army plans to support the U.S. Cyber Command through the Army Forces Cyber, and the Marine Corps established Marine Forces Cyber.

DOD officials we interviewed expressed varying opinions on whether the establishment of the U.S. Cyber Command will help DOD better address cybersecurity threats. Many officials with whom we spoke said that it was a step in the right direction as the command will potentially provide a single point of accountability for cyber-related issues. Additionally, the Joint Staff concluded that a four-star subunified Cyber Command under U.S. Strategic Command, dual-hatted as the Director of the National Security Agency, would be the most effective way to address the need to better integrate cyber defense, attack, exploitation, and network

operations. However, officials from some combatant commands expressed concern about the command's close relationship to the DOD intelligence community. These officials believed that with the Director of the National Security Agency dual-hatted as the Commander of U.S. Cyber Command, the U.S. Cyber Command will become too focused on intelligence structures in detriment to a focus on operations in support of the combatant commands. Additionally, DOD officials expressed some concern regarding the reduced role of the Defense Information Systems Agency with respect to the U.S. Cyber Command. The agency head was previously also the Commander of the Joint Task Force–Global Network Operations. Under the new relationship, the Defense Information Systems Agency will continue to provide network and information assurance technical assistance through a field office and a support element at U.S. Cyber Command.

DOD Recognizes the Need to Update Cyber-Related Joint Doctrine and Guidance, but Lacks a Timetable for Completion

Several joint doctrine publications address aspects of cyberspace operations, but DOD officials acknowledge that this is insufficient. None of the joint publications that mention “cyberspace operations” contains a sufficient discussion of cyberspace operations. DOD doctrine also lacks key common definitions. DOD recognizes the need to develop and update cyber-related joint doctrine and is currently debating the merits of developing a single cyberspace operations joint doctrine publication in addition to updating all existing doctrine. However, there is no timetable for completing the decision-making process or for updates to existing doctrine.

Numerous Joint Doctrine Publications Discuss Cyber-Related Topics, but Need Updating

DOD has numerous joint doctrine publications that discuss cyber-related topics; however, the content is incomplete or out of date and DOD lacks joint doctrine that fully addresses cyberspace operations. The discussion of cyber-related topics in current joint doctrine publications is limited and insufficient, leaving problems such as incomplete definitions. Other discussions—such as what constitutes a cyber force—are not uniformly defined across DOD doctrine publications and guidance. DOD recognizes the need to develop and update cyber-related joint doctrine and is currently debating the merits of developing a single, overarching cyber joint doctrine publication in addition to updating all existing doctrine with respect to cyberspace operations. However, DOD has not set a timetable for the completion of these efforts.

According to DOD, the purpose of joint doctrine is to enhance the operational effectiveness of U.S. forces.³³ Joint doctrine consists of fundamental principles to guide the employment of U.S. military forces in coordinated action toward a common objective and should include key terms, tactics, techniques, and procedures. In order to be effective, combatant commands and military services need to understand the joint functions within the domain and the manner in which those joint functions are integrated globally as well as operationally. The cyberspace domain is inherently joint; it cuts across all combatant commands, military services, and agency boundaries and supports engagement operations for all geographic combatant commands. Therefore, DOD expects that a joint publication focusing on all aspects of cyberspace operation will not only enhance the operational effectiveness and performance of joint U.S. forces but also provide a doctrinal basis for collaborative planning and interagency coordination.

DOD determined that it has addressed cyberspace-related topics in at least 16 DOD joint doctrine publications and mentions “cyberspace operations” in at least 8 joint publications. This reflects the importance of cyber-related issues across the body of joint doctrine. However, according to combatant command officials, the discussions and content in these publications are insufficient and do not completely address cyberspace operations or contain critical related definitions. U.S. Joint Forces Command’s assessment of the existing state of joint doctrine for cyber issues concluded that while the term “cyberspace operations” was addressed or mentioned in 8 approved and draft publications, none contained a significant discussion of cyberspace operations.³⁴

U.S. Joint Forces Command’s assessment of DOD joint publications showed that the majority of references to cyberspace operations come from Joint Publication 3-13, *Information Operations*—the current publication with the most relevance to cyber issues.³⁵ While this publication may have been sufficient for its intended purposes at the time it was written in 2006, U.S. Strategic Command reported that

³³Chairman, Joint Chiefs of Staff, Instruction 5120.02B, *Joint Doctrine Development System*.

³⁴U.S. Joint Forces Command, *Front End Analysis* (Norfolk, Va., September 2009).

³⁵Chairman, Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations*.

Information Operations should be revised to use updated cyberspace terminology and content.³⁶ U.S. Strategic Command reported that the publication is not currently sufficient and does not provide a basis for cyberspace joint doctrine for 3 key reasons. First, its definition of cyberspace does not reflect the scope of the current definition of cyberspace that was approved by the Deputy Secretary of Defense in May 2008.³⁷ The definition in the publication restricts cyberspace to “digital information communicated over computer networks,” while the current approved definition recognizes cyberspace as a global domain within the information environment that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.³⁸ Second, the publication discusses computer network operations as a component of information operations by grouping it with military deception, operation security, psychological operations, and electronic warfare; but it does not recognize the scope of computer network operations as a warfighting domain. Third, Joint Publication 3-13 omits integral elements in the discussion of computer network operations that are important to provide a complete view and scope of cyberspace operations. For example, the publication discusses computer network attack and computer network defense but does not thoroughly address key elements such as computer network defense response actions, computer network attack—operational preparation of the environment, or network operations. Our analysis of the current usage of cyber-related terms confirms that these are considered important elements of both computer network operations and cyberspace operations.

DOD Lacks a Common Definition of Cyber Personnel

Another example of the shortfall in existing doctrine is the lack of a common definition for what constitutes cyber personnel in DOD. According to a U.S. Joint Forces Command report, the cyberspace operations community lacks a common dictionary of terms, and the terms

³⁶U.S. Strategic Command Memorandum, *Joint Doctrine for Cyberspace Operation Project Proposal* (Offutt Air Force Base, Neb., May 11, 2009).

³⁷Deputy Secretary of Defense Memorandum, *The Definition of Cyberspace* (Washington, D.C., May 12, 2008).

³⁸However, the most recent Joint Publication 3-0, *Joint Operations*, updated March 22, 2010, does define cyberspace and cyberspace operations with the most current definitions.

defined in current doctrine are not used uniformly.³⁹ This can cause confusion in planning for adequate types and numbers of personnel. Because career paths and skill sets are scattered across various career identifiers, the military services and commands vary in their scope and definitions of what constitutes cyber personnel. As a result, there are cases in which the same cyber-related term may mean something different among the services. In another report, the U.S. Joint Forces Command found that 18 different cyber position titles across combatant commands are used to identify cyberspace forces.⁴⁰ Some of these titles may be inconsistent from command to command and are likely to be duplicates. According to the report, U.S. Pacific Command had the largest number of cyber personnel positions and position titles compared to other combatant commands, while some commands reported no cyber personnel. This may be due in part to duplicative and differing definitions among the combatant commands of what constitutes cyber personnel. Examples of cyberspace-related position titles from combatant commands include

- Computer Network Attack Intelligence Officer,
- Computer Network Attack Ops Officer,
- Computer Network Attack Ops Planner,
- Computer Network Attack Planner,
- Computer Network Attack Weapons Risk Assessor,
- Computer Network Defense Planner,
- Computer Network Operations Exercises Officer,
- Computer Network Operations Planner,
- Computer Network Operations Technician,
- Information Assurance Support Person,
- Intelligence Support to Computer Network Attack,
- Intelligence Support to Computer Network Defense,
- Intelligence Systems Officer / Computer Network Defense,
- Network Attack Planner,
- Network Defender,
- Network Defense Planner,
- Network Warfare Planner, and

³⁹U.S. Joint Forces Command, *Cyber Defense Limited Objective Experiment Final Report, Version 1.2* (Norfolk, Va., Nov. 30, 2009).

⁴⁰U.S. Joint Forces Command, *Lead.1 Final Report* (Norfolk, Va., September 2008).

-
- Planner Analyst.⁴¹

The lack of clear guidance on cyber personnel in joint doctrine is also reflected in the military services. The military services do not currently have specific job identifiers for cyberspace operations, and cyberspace-related jobs are generally identified under the umbrella of intelligence, communication, or command and control. While the military services bring unique capabilities based upon their individual core competencies, cyberspace forces must meet joint standards. U.S. Joint Forces Command, whose mission is to synchronize global forces, reported that it is unable to quickly and easily identify personnel who are certified for cyber operations, as there is no identifier in the personnel records that indicate if the individual is a “cyber warrior.” Additionally, U.S. Strategic Command reviewed current military service cyber force identifiers and reported that the Air Force identifies computer-related careers under “general” for enlisted personnel and under “non-technical” skills for officers; the Navy identifies computer network operation careers under “information warfare” for officers and “information systems technicians” or “intelligence and communications” for enlisted personnel.

DOD Recognizes the Need to Update and Improve Cyber-Related Joint Doctrine but Lacks a Timetable for Completion

DOD recognizes the need to update and improve cyber-related joint doctrine. According to DOD, joint doctrine is being revised and updated and will include refined discussion of cyber-related issues. The U.S. Joint Forces Command’s assessment of the status of cyber-related joint doctrine reported that 14 of the 16 publications that discuss cyberspace-related issues are in various stages of review or revision and that virtually all will contain additional information that is consistent with the new definitions for cyberspace and cyberspace operations. The report also states that while pending revisions to various joint publications could provide the necessary coverage of these topics, the degree of coverage is not known until the draft revisions are available for review and comment.⁴²

The military services have also developed tactics, techniques, and procedures that have helped them understand and conduct cyber operations and bridge the gap until broader authoritative policy and

⁴¹Ibid.

⁴²U.S. Joint Forces Command, *Front End Analysis*.

doctrine are completed. However, until the revised doctrine publications are released, the full extent of the changes and their inclusion of cyber-related information will be unknown. While all of these efforts represent significant progress toward enhancing joint doctrine, there is no timetable for the completion of all cyber-related updates to existing joint publications.

DOD is also currently debating the merits of developing a single, overarching cyber joint doctrine publication in addition to updating all existing doctrine. Separate joint doctrine publications are devoted to other major elements of operations in various “domains,” including such topics as mine warfare, amphibious operations, urban operations, operations other than war, counterdrug operations, and space operations.

In 2007 the *National Military Strategy for Cyberspace Operations Implementation Plan* tasked a number of DOD commands and organizations with cyber-related studies, some of which evaluated cyber-related joint doctrine.⁴³ There has subsequently been broad agreement within DOD about the need for improved joint doctrine. However, not all commands agreed about the need for a separate cyber-specific doctrine publication. Table 4 provides examples of some of the conclusions and recommendations stemming from studies related to cyber joint doctrine.

⁴³DOD, *National Military Strategy for Cyberspace Operations Implementation Plan*.

Table 4: Examples of DOD Studies Related to Cyber Joint Doctrine

Study	Conclusion
Joint Chiefs of Staff, Quadrennial Roles and Missions Team, Awareness and Assessments Group, <i>Actors, Technologies, Threats, Challenges, and Assessments in Cyberspace</i> , August 2008	Recommended that DOD adopt a joint approach to cyberspace force development, training, personnel assignment, and equipping to reflect the fact that cyberspace is a joint warfighting domain.
U.S. Strategic Command, National Security Agency, and Central Security Service, <i>Joint Doctrine-Organization-Training-Materiel-Leadership-Personnel-Facilities Change Recommendation for Cyber Operations (Draft)</i> , 2008 ^a	Recommended that U.S. Strategic Command lead cyberspace doctrine development within Joint Staff doctrine development process. Build cyberspace doctrine using unit and operational experience.
U.S. Strategic Command and Joint Staff, <i>Doctrine.1</i> , 2009	Recommended definitional changes to current joint publications and that DOD continue to develop a joint doctrine publication for cyber operations.
U.S. Joint Forces Command, <i>Lead.1</i> , 2008	Recommended that Joint Staff develop and synchronize joint cyberspace operations doctrine based on current joint publications and that it resolve disparities and gaps in cyberspace definitions.
U.S. Joint Staff, <i>Planning.2</i> , 2008	Enhance cyber-related content in joint doctrine and DOD and Joint Staff policy. Joint doctrine community must work to harmonize cyber-related discussions through all applicable joint publications undergoing revision.

Source: GAO review of DOD Information.

^aU.S. Strategic Command, National Security Agency, and Central Security Service, *Joint Doctrine-Organization-Training-Materiel-Leadership-Personnel-Facilities Change Recommendation for Cyberspace Operations (Draft)*, (Washington, D.C., October 2008).

In May of 2009, U.S. Strategic Command proposed the development of an overarching joint publication for cyberspace operations dedicated to all aspects of cyberspace operations.⁴⁴ As the DOD command responsible for evaluating joint doctrine proposals, U.S. Joint Forces Command conducted a *Front End Analysis* that reviewed and analyzed the proposal to determine if a doctrinal void exists and if the proposal is appropriate for inclusion in the doctrine community.⁴⁵ Additionally, the U.S. Joint Forces Command officials we spoke with expressed concern about developing a separate cyber joint publication and that this might create inefficiencies and disconnects with existing related doctrine in such areas as information operations. The *Front End Analysis* recommended that further consideration of a separate joint doctrine publication be postponed and that U.S. Strategic Command develop a joint test publication for cyberspace operations.

⁴⁴U.S. Strategic Command, *Joint Doctrine for Cyberspace Operation Project Proposal*.

⁴⁵U.S. Joint Forces Command, *Front End Analysis*.

In September 2009, the Joint Staff approved the development of the cyberspace operations joint test publication. A joint test publication is a proposed version of a joint doctrine that normally contains contentious issues.⁴⁶ After the test publication is developed, it will be evaluated through U.S. Joint Forces Command, resulting in one of the following recommendations: (1) that DOD convert the cyber joint test publication into a joint publication; (2) that DOD incorporate the joint test publication or portions of it into existing joint publications; or (3) that DOD determine that the cyber joint test publication is not sufficient and discontinues work on it with no effect on joint doctrine.⁴⁷ A test publication is not considered approved doctrine. The Joint Staff established a milestone of June 2010 for completion of the draft test publication. The Joint Staff told us it expects evaluation of the test publication to take 6 to 12 months. However, DOD has not determined a completion date for the evaluation or for the final decision on the joint test publication as part of the test publication development plan.

Regardless of whether DOD proceeds with developing a separate joint doctrine, completion of its effort to update existing doctrine is crucial to further improve the understanding of key cyber-related terms and operational issues throughout DOD. According to DOD's principal guidance for joint doctrine development, joint doctrine must evolve as the United States strives to meet national security challenges, and doctrinal voids are identified.⁴⁸ Providing a baseline of common definitions and operational constructs for cyber operations in existing doctrine or in a separate overarching publication would provide the basis for future adaptation. DOD's well-established joint doctrine development processes provides a sound structure to assess all aspects of cyber operations, propose doctrinal change or creation, and establish clear time frames for completing interim and final efforts. The lack of a time frame for cyber doctrine makes it difficult for DOD to plan for additional efforts that rely on doctrine and may permit delay while service and joint officials continue to

⁴⁶According to the Chairman of the Joint Chiefs of Staff in Instruction 5120.02B, *Joint Doctrine Development System*, a Joint Test Publication is used to "field test" a validated concept to ensure it is appropriately vetted before incorporation in joint doctrine.

⁴⁷Chairman, Joint Chiefs of Staff, Instruction 5120.02B, *Joint Doctrine Development System*.

⁴⁸Chairman, Joint Chiefs of Staff, Instruction 5120.02B, *Joint Doctrine Development System*.

debate the possible future of cyber operations rather than concentrate on establishing a solid basis upon which future efforts can be built.

Conflicting Guidance and Unclear Responsibilities Have Created Challenges for Command and Control of Cyberspace Operations

DOD has assigned authorities and responsibilities for implementing cyberspace operations among combatant commands, military services, and defense agencies. However, the supporting relationships necessary to achieve command and control of cyberspace operations remain unclear. In response to a major computer infection in 2008, U.S. Strategic Command identified confusion regarding command and control authorities and chains of command because the exploited network fell under the purview of both its own command and a geographic combatant command. DOD-commissioned studies have recommended command and control improvements.

Cyber Command and Control Is Unclear and Divided among DOD Components

Lines of command and control of cyber forces are divided among U.S. Strategic Command, the geographic combatant commands, and the military services, through several policy and guidance documents. The *National Military Strategy for Cyberspace Operations*,⁴⁹ the 2008 Unified Command Plan,⁵⁰ DOD Directive O-8530.1,⁵¹ and the Standing Rules of Engagement⁵² are all relevant to command and control of cyberspace operations, but they sometimes conflict with each other and remain unclear because of overlapping responsibilities.

The *National Military Strategy for Cyberspace Operations*, issued in December 2006, demonstrates DOD's recognition that clear command and control relationships are necessary for the successful application of military power in cyberspace. The purpose of this strategy is to establish

⁴⁹Chairman, Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*.

⁵⁰DOD, *Unified Command Plan* (Washington, D.C., Dec. 17, 2008).

⁵¹DOD, Directive O-8530.1, *Computer Network Defense* (Washington, D.C., Jan. 8, 2001).

⁵²Chairman, Joint Chiefs of Staff, Instruction 3121.01B, *Standing Rules of Engagement / Standing Rules for the Use of Force for U.S. Forces* (Washington, D.C., June 18, 2008). Rules of engagement are the directives issued by competent military authority that delineate the circumstances and limitations under which U.S. forces will initiate, continue, or both, combat engagement with other forces they encounter.

a common understanding of cyberspace and set forth a military strategic framework that orients and focuses DOD action in the areas of military, intelligence, and business operations in and through cyberspace. According to the strategy, the United States can achieve superiority in cyberspace only if command relationships are clearly defined and executed, and must support unity of effort in achieving combatant commanders' missions as well as maintaining freedom of action in cyberspace. The strategy also states that cyberspace provides the foundation for command and control of military operations in other domains and that, due to the nature of cyberspace, command and control requires extremely short decision-making cycles. According to the strategy, effective command and control integrates, deconflicts, and synchronizes cyberspace operations at the speeds required for achieving awareness and generating effects, while failure to establish an integrated structure can hinder collaboration and lengthen decision-making cycles.

The 2008 Unified Command Plan gave specific responsibilities for synchronizing planning for cyberspace operations to U.S. Strategic Command, including directing global information grid operations and defense, planning against designated cyberspace threats, coordinating with other combatant commands and U.S. government agencies, and executing cyberspace operations. The Unified Command Plan also states that, unless otherwise directed, combatant commanders will exercise command authority over all commands and forces assigned to them, in accordance with section 164 of title 10 of the U.S. Code. However, while individual service networks may reside within the area of responsibility of a particular geographic combatant command, that geographic commander does not possess the authority to direct the network operations of his component organizations, because those component networks are owned and directed by their respective service organizations through their role as Computer Network Defense Service Providers (defined within DOD Directive O-8530). This establishes a conflicting situation that affects the geographic combatant commanders' visibility over networks in their areas of responsibility.

Also, the Standing Rules of Engagement state that unit commanders always retain the inherent right and obligation to exercise unit self-defense in response to a hostile act or demonstrated hostile intent. This generally extends to commanders conducting information operations and includes the authorization to conduct protective, defensive, and restorative measures for the networks they control in response to all unauthorized network activity. However, when defensive measures would have potentially adverse effects across multiple DOD networks or on

adversary or intermediary networks outside the DOD global information grid, they must be approved by the Commander of U.S. Strategic Command, under his responsibility for DOD-wide network operations, and coordinated with affected components and appropriate law enforcement or intelligence organizations.

2008 Cyber Incident Exposed Weaknesses in DOD's Command and Control Authorities and Procedures for Cyberspace Operations

An incident of malware infection on DOD systems in 2008 illustrated that a lack of operational clarity significantly slowed down DOD's response. As a result of this malware eradication effort, U.S. Strategic Command identified confusion regarding the exploited networks. This led to uncoordinated, conflicting, and unsynchronized guidance in response to the incident being issued in several forms via multiple channels. Our review confirmed that multiple directives contributed to confusion at the execution level, leaving operators and administrators to reconcile priorities and question which procedures were appropriate and most urgent to address the malware infection. Although DOD intends for the new U.S. Cyber Command to facilitate command and control, as late as December 2009, DOD noted that these problems had not been fully addressed, though the new U.S. Cyber Command is expected to be established by October 2010. Without complete and clearly articulated guidance on cyber command and control responsibilities that is well-communicated and practiced with key stakeholders, DOD may have difficulty in building unity of effort for carrying out cyber operations.

DOD-Commissioned Studies Recommend Cyber Command and Control Improvements

DOD has recognized the need for improvements in its command and control organization for cyberspace operations and commissioned associated studies by U.S. Joint Forces Command⁵³ and the Institute for Defense Analyses.⁵⁴ Both classified studies evaluated DOD's command and control organization and recommended improvements in 2008.

DOD has started to act on these recommendations, by initiating key organization changes, such as establishing the U.S. Cyber Command. However, until DOD updates its policies and guidance to clarify command and control relationships for cyber operations and clearly communicates

⁵³U.S. Joint Forces Command, *Lead.1 Final Report*.

⁵⁴Institute for Defense Analyses, *Independent Assessment Panel: Command and Control Structures and Authorities for Cyber Operations* (Alexandria, Va., September 2008).

those to all DOD entities, its efforts to conduct coordinated and timely actions to defend DOD's critical networks and other cyber operations will be degraded.

DOD Has Identified Some Capability Gaps in Cyber Operations, but Lacks a Comprehensive Assessment of Departmentwide Cyberspace Needs and an Implementation Plan to Address Any Gaps

DOD has identified some cyberspace capability gaps. DOD also continues to study the extent of these gaps. However, it has not completed a comprehensive, departmentwide assessment of needed resources associated with the capability gaps and an implementation plan to address any gaps.

DOD Has Identified Some Capability Gaps in Cyber Operations

According to the 2006 *National Military Strategy for Cyberspace Operations*, military departments and certain agencies and commands should develop the capabilities necessary to conduct cyberspace operations, including consistently trained personnel, infrastructure, and organization structures. U.S. Strategic Command's *Operational Concept for Cyberspace* reported in 2008 that national security vulnerabilities inherent in cyberspace make it imperative that the United States develop the requisite capabilities, policy, and tactics, techniques, and procedures for employing offensive, defensive, and supporting operations to ensure freedom of action in cyberspace. In addition, a study commissioned by the Joint Staff and conducted by the Institute for Defense Analyses states that the key underlying drivers of effectiveness in cyberspace are developing and deploying the right tools and building and sustaining an adequate cyber force of trained and certified people.⁵⁵ Institute for

⁵⁵Institute for Defense Analyses, *Independent Assessment Panel: Command and Control Structures and Authorities for Cyber Operations* (Alexandria, Va., September 2008).

Defense Analyses officials stated that unless DOD has adequate resources for cyber operations, organizational changes within the cyber domain will not be effective.

DOD commands have identified capability gaps that hinder their ability to marshal resources to operate in the cyberspace domain. U.S. Strategic Command and other combatant commands highlighted their cyber capability gaps in their Integrated Priority Lists for fiscal years 2011-2015.⁵⁶ U.S. Strategic Command, which is tasked with being the global synchronizer for cyber operations within DOD, identified in its Integrated Priority List for fiscal years 2011-2015 gaps and associated priorities in such areas as the need to be able to defend against known threats, detect or characterize evolving threats, and conduct exploitation and counter operations, as desired. U.S. Strategic Command listed cyber-related gaps as its highest priority, emphasizing the need for and importance of resources to increase cyber capabilities. U.S. Pacific Command, U.S. Special Operations Command, and U.S. Joint Forces Command have also reported cyber capability gaps involving lack of sufficient numbers of trained personnel to support their cyber operations and a need for additional cyber intelligence capabilities.

U.S. Strategic Command has reported that the lack of cyber resources it identified has affected the command's ability to respond to requests for cyber capabilities from other combatant commands, particularly for full-spectrum cyberspace operations. It remains to be seen what effect the newly proposed U.S. Cyber Command will have on this process, particularly with Joint Functional Component Command for Network Warfare and Joint Task Force–Global Network Operations being merged into one organization within the new U.S. Cyber Command.

A need for more cyber planners and cyber-focused intelligence analysts was a common theme during our meetings with officials at the combatant commands. Officials at several of the geographic combatant commands stated that without the proper planners and cyber-focused intelligence analysts, they lacked situational awareness of their networks and the

⁵⁶Combatant commanders annually submit capability needs prioritized across service and functional lines that define capability shortfalls that limit combatant commander assigned mission accomplishment.

ability to both plan cyber operations for their respective commands and request applicable support from U.S. Strategic Command. For example, cyber planners play a key part in the developmental process of a computer network attack operation. U.S. Central Command officials stated that although most computer network attack operations are being conducted in its area of responsibility, it does not have a single full-time dedicated cyber planner to assist in the development of such operations. Because it lacks the appropriate trained personnel and dedicated career path, U.S. Central Command has redirected personnel with cyber expertise to act as temporary planners. This greatly affected the command's ability to match resources to, and plan for, all cyber-related functions. For example, a cyber planner within U.S. Central Command was borrowed from another career field, worked as a planner for a time, and then was reassigned to help resolve information technology issues at a help desk.

Without a sufficient number of cyber planners in-theater, combatant commands will continue to struggle with being able to plan cyber activities to assist in accomplishing the commander's mission objectives, and communicating their need for assistance to U.S. Strategic Command. The lack of skilled and highly trained cyber personnel presents challenges for many DOD components, and the lack of sufficient personnel prevents DOD components from fulfilling essential computer network operation activities.

DOD Is Taking Steps to Study Cyber Capability Gaps but Lacks a Comprehensive Departmentwide Capabilities-Based Assessment

DOD's Joint Capabilities Integration and Development System provides a framework from which DOD can assess and prioritize departmentwide cyber-related capability gaps, assign responsibility for addressing them, and develop an implementation plan for achieving and tracking results. This system is DOD's primary means of identifying the capabilities required to support national strategies.⁵⁷ It therefore helps the military services prepare long-term program plans to address critical joint capabilities. One of the key elements of this system is a capabilities-based assessment that defines a mission, identifies required capabilities, identifies gaps, assesses risk associated with those gaps, prioritizes

⁵⁷Chairman, Joint Chiefs of Staff, Instruction 3170.01G, *Joint Capabilities Integration and Development System* (Washington, D.C., Mar. 1, 2009).

gaps, assesses nonmateriel solutions, and recommends actions for the department to pursue.

While the department's review of cyberspace capability gaps and various studies on cyberspace operations are steps in the right direction, it remains unclear whether these gaps will be addressed, since DOD has not conducted the kind of comprehensive capabilities-based assessment outlined in the Joint Capabilities Integration and Development System or established an implementation plan to resolve any resulting gaps. For example, DOD conducted an assessment of computer network defense and computer network attack capability gaps in 2004 that highlighted the need for a broader effort to address gaps as part of the Joint Capabilities Integration and Development System.⁵⁸ However, this assessment was not finalized for action.

DOD has since conducted individual cyber-related studies focused on the lack of trained cyber personnel and also brought attention to cyber-related capability gaps listed in the combatant commanders' fiscal year 2011-2015 Integrated Priority Lists. In February 2009, the Joint Staff directed the Force Support Functional Capabilities Board to address future cyberspace force manning and organization gaps and to develop a current baseline manpower posture across cyberspace operations and present a consolidated view of all documented DOD cyberspace manpower requirements.⁵⁹ The Force Support Functional Capabilities Board put together a Cyberspace Study Team to engage the combatant commands, services, and agencies in their efforts.

In addition to the cyberspace studies discussed above, and as part of DOD's Joint Capabilities Integration and Development System, the Joint Requirements Oversight Council issued a memorandum in June 2009 (JROCM 113-09) that reviewed and endorsed 85 capability gaps across DOD from the combatant commands' reported Integrated Priorities Lists—4 of which were cyber-related. Throughout the Joint Capabilities Integration and Development System process, functional capabilities boards provide oversight and assessment, as appropriate, to ensure

⁵⁸U.S. Strategic Command, *Capstone Requirements Document for Computer Network Defense and Computer Network Attack* (Jan. 13, 2004), draft.

⁵⁹The Functional Capabilities Boards use the Integrated Priority Lists while assessing mitigation strategies to meet the combatant commander's needs.

system documents take into account joint capabilities and alternative approaches to solutions. In this case, the memorandum stated that Functional Capabilities Boards will track the recommendations related to the capability gaps.

The Functional Capabilities Boards periodically report on the way ahead for recommended actions and report recommendations to the Joint Requirements Oversight Council for decision. The Joint Requirements Oversight Council's approval and implementation in a Joint Requirements Oversight Council Memorandum serves as the analytic underpinning for many future decisions related to capability gaps. However, capability gaps are considered "closed" based on the Joint Requirements Oversight Council's decisions and the assumption that those decisions will be implemented. Failure to execute the Joint Requirements Oversight Council's decision is not considered a capabilities gap assessment issue, although it may generate an input for the next capabilities gap assessment cycle.

DOD has continued to make progress with respect to some of the individual capability gaps identified from the Integrated Priority Lists for fiscal year 2011-2015. Also the memorandum requested that U.S. Strategic Command lead the joint effort to create a concept of operations to inform future decisions but provided no specific time frame for these actions in the memorandum.

Joint Staff officials we interviewed recognized that fully addressing the cyber capability gaps they have thus far identified may take years to complete. Some cyber capability gaps are relatively new, thus the Joint Requirements Oversight Council has deferred manpower studies to be completed first so that informed decisions can be made at a later time. For example, the Joint Staff officials also noted that some cyber-related resource requests involving computer network operations from U.S. Pacific Command could not be addressed immediately because of the lack of existing doctrine or policy on the appropriate authority to carry out this specific action.

While the Joint Staff's action to direct the Functional Capabilities Boards to track progress toward addressing capability gaps is a step in the right direction for developing a plan to address capability gaps, it remains unclear whether or when these gaps will be addressed. For example, as of December 2009, the Joint Staff listed all the cyber-related capability gaps noted by Joint Requirements Oversight Council Memorandum 148-

09 as closed; but for several of the gaps, the memorandum only cited the manpower study discussed above as rationale.

Furthermore, the Joint Staff is also currently reviewing the most recent Integrated Priority List from the combatant commands for fiscal years 2012-2017, in which some previously-cited cyber capability gaps were repeated.⁶⁰

Though DOD has previously begun efforts similar to a comprehensive capabilities-based assessment for cyberspace, it has not completed those efforts. The studies we discuss and ongoing efforts, such as the individual Functional Capabilities Board actions, provide much-needed information to DOD officials about where further action may be needed. But these efforts lack the scope of a complete capabilities-based assessment and do not include time frames or a funding strategy for addressing capability gaps. Further, in prior work, we found that best practices for strategic planning have shown that effective and efficient operations require detailed plans outlining major implementation tasks, defined metrics and timelines to measure progress, a comprehensive and realistic funding strategy, and communication of key information to decision makers.⁶¹ Absent such elements as a broad assessment of cyber-related capability gaps, time frames for assessing and addressing gaps, and a strategy for funding any required programs, combatant commands are compelled to report the same capability gaps they had in previous years without an assurance that they will be addressed; and the military services will be unable to fully plan for programs to address cyberspace requirements. As a result, cyber capability gaps across DOD will continue to hinder DOD's ability to plan for and conduct effective cyber operations.

Conclusions

DOD has been characterized as one of the best-prepared federal agencies to defend against cybersecurity threats, but keeping pace with

⁶⁰For the purpose of this report, we reviewed DOD efforts to address capability gaps identified in the Integrated Priority Lists for fiscal years 2011-2015. DOD began its review of the combatant commands' Integrated Priority Lists for fiscal year 2012-2017 in January 2010. It was too early in the Joint Staff review process to include this in our analysis of DOD actions to address these capability gaps.

⁶¹GAO, *Reserve Forces: Army Needs to Finalize an Implementation Plan and Funding Strategy for Sustaining an Operational Reserve Force*, [GAO-09-898](#) (Washington, D.C., Sept. 17, 2009).

the magnitude of cybersecurity threats DOD faces currently and will face in the future is a daunting prospect. DOD networks and our country's critical infrastructure can be disrupted, compromised, or damaged by a relatively unsophisticated adversary and, as witnessed by the 2008 infections from removable media, this can potentially affect the conduct of military operations. The U.S. military is dominant in the land domain, unchallenged in the air, and has few near-peers in the maritime domain. However, the technical and economic barriers to entry into the cyber domain are much lower for adversaries and as a result place U.S. networks at great risk. DOD has taken many important steps to better organize its cyber efforts with the creation of the U.S. Cyber Command, but it is too early to tell whether this will provide the necessary leadership and guidance DOD requires to address cybersecurity threats. Based on public statements from DOD senior leadership, DOD understands the severity of the problem. DOD's actions to reassess its organization for cyber-related operations, assess and update joint doctrine, assess command and control relationships, and study cyber-related capability gaps all take advantage of DOD's considerable planning and operational experience. The next step to keep pace or stay ahead of the rapidly-changing environment reflected by the cyber domain is for DOD to further its efforts in each of these areas in a more comprehensive manner and as part of a cohesive policy.

Recommendations for Executive Action

To strengthen DOD's cyberspace doctrine and operations to better address cybersecurity threats, we recommend that the Secretary of Defense take the following two actions:

- direct the Chairman of the Joint Chiefs of Staff in consultation with the Under Secretary of Defense for Policy and U.S. Strategic Command to establish a time frame for (1) deciding whether or not to proceed with a dedicated joint doctrine publication on cyberspace operations and for (2) updating the existing body of joint doctrine to include complete cyberspace-related definitions, and
- direct the appropriate officials in the Office of the Secretary of Defense, in coordination with the Under Secretary of Defense for Policy and the Joint Staff, to clarify DOD guidance on command and control relationships between U.S. Strategic Command, the services, and the geographic combatant commands regarding cyberspace operations, and establish a time frame for issuing the clarified guidance.

To ensure that DOD takes a more comprehensive approach to its cyberspace capability needs and that capability gaps are prioritized and addressed, we make two additional recommendations, that the Secretary of Defense direct the appropriate Office of the Secretary of Defense officials, in coordination with the secretaries of the military departments and the Joint Chiefs of Staff, to

- develop a comprehensive capabilities-based assessment of the departmentwide cyberspace-related mission and a time frame for its completion, and
- develop an implementation plan and funding strategy for addressing any gaps resulting from the assessment that require new capability development or modifications to existing programs.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD agreed with our 4 recommendations and discussed some of the steps it is taking and planning to take to address these recommendations. DOD also provided technical comments, which we have incorporated into the report where appropriate.

In response to our recommendation that the Secretary of Defense direct the Chairman of the Joint Chiefs of Staff in consultation with the Under Secretary of Defense for Policy and the U.S. Strategic Command to establish a time frame for deciding whether or not to proceed with a dedicated joint doctrine publication on cyberspace operations and for updating the existing body of joint doctrine to include complete cyberspace-related definitions, DOD agreed and stated that as part of implementing the National Military Strategy for Cyberspace Operations, an assessment of joint doctrine is under way and is expected to be completed by the end of fiscal year 2011. Furthermore, DOD said that this process will also include related cyber lexicon and definitions. While our report was in final processing, DOD began to publish some of the doctrinal updates they had agreed needed to be made. Since the National Military Strategy for Cyberspace Operations was published in 2006, we believe the new joint doctrine assessment represents progress that should help DOD address some of the existing gaps in joint doctrine with a time frame for completing the effort. We continue to believe that DOD's overall assessment should include a decision on whether or not to proceed with a dedicated joint doctrine publication on cyberspace operations and a plan for updating the existing body of joint doctrine.

DOD agreed with our recommendation that it clarify roles and responsibilities, including command and control relationships between the U.S. Strategic Command, the services, and the geographic combatant commands regarding cyberspace operations, and establish a time frame for issuing the clarified guidance. However, DOD stated it had already satisfied this recommendation by means of the June 23, 2009, memorandum establishing U.S. Cyber Command and the 2008 Unified Command Plan. According to DOD, both documents have promulgated clear guidance for command and control relationships.⁶² The Secretary of Defense memorandum establishing the U.S. Cyber Command does allude to the U.S. Cyber Command implementation plan, which does contain some information on command and control relationships, but does not provide the kind of clear guidance we describe as lacking in our report. The implementation plan further alludes to a U.S. Cyber Command Concept of Operations that will be published at a later date, which may provide further information on command and control guidance. While the 2008 Unified Command Plan discusses missions and responsibilities for U.S. Strategic Command in cyberspace operations, we believe this information is outdated, considering the memo directing the establishment of U.S. Cyber Command was issued in June 2009. Although it is early in the establishment process for the new U.S. Cyber Command, we continue to believe that DOD should take advantage of opportunities to develop and articulate clear command and control guidance that will provide a timely and cohesive approach to combating cyber threats throughout the chain of functional and geographic combatant commands, the services, and other DOD components in anticipation of the U.S. Cyber Command reaching full operating capability in October 2010. Vehicles for conveying this guidance might include the U.S. Cyber Command Concept of Operations, additional implementation plans, and revisions to the Unified Command Plan.

DOD agreed with our recommendation that the Secretary of Defense direct the appropriate Office of the Secretary of Defense officials, in coordination with the Secretaries of the military departments and the Joint Chiefs of Staff, to develop a comprehensive capabilities-based assessment of the departmentwide cyberspace-related mission and a

⁶²The Secretary of Defense, *Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operation* (Washington, D.C., June 23, 2009) and DOD, *Unified Command Plan 2008* (Washington, D.C., Oct. 3, 2008).

time frame for its completion. DOD indicated that cyber defense would be one focus area for risk management decisions as part of the upcoming budget cycle but provided no further information on how it planned to implement the steps in the recommendation. We recognize that fully addressing DOD's cyber capability gaps will take years; however, we maintain the importance of establishing an assessment of these gaps and establishing a time frame to address them.

DOD agreed with our recommendation that the Secretary of Defense direct the appropriate Office of the Secretary of Defense officials, in coordination with the Secretaries of the military departments and the Joint Chiefs of Staff, to develop an implementation plan and funding strategy for addressing any gaps resulting from the assessment that require new capability development or modifications to existing programs. DOD stated that its budget risk management decisions, as well as the development of a National Defense Strategy for Cyberspace Operations would help the department identify and mitigate gaps but provided no further information on how they planned to implement the steps identified in the recommendation. We continue to believe it is important to develop an implementation plan and funding strategy for addressing these gaps in order to avoid combatant commands reporting the same capability gaps they had in previous years without an assurance that they will be addressed and that the military services will be unable to fully plan for programs to address cyberspace requirements. Without this effort, cyber capability gaps across DOD will continue to hinder its ability to plan for and conduct effective cyber operations.

DOD's comments are reproduced in full in appendix V.

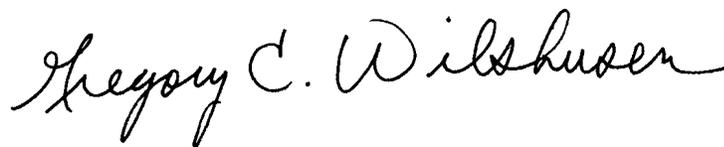
We are sending copies of this report to appropriate congressional committees. We are also sending copies to the Secretary of Defense and the Chairman, Joint Chiefs of Staff. In addition, the report will be available at no charge on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions concerning this report, please contact Davi M. D'Agostino at (202) 512-5431 or Gregory C. Wilshusen at (202) 512-6244. We can also be reached by e-mail at dagostinod@gao.gov or wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on

the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.



Davi M. D'Agostino
Director
Defense Capabilities and Management



Gregory C. Wilshusen
Director
Information Security Issues

List of Requesters

The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable W. "Mac" Thornberry
Chairman
The Honorable James R. Langevin
Ranking Member
Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
House of Representatives

Appendix I: Objectives, Scope, and Methodology

To address our objectives, we focused our work on the Department of Defense's (DOD) organizations that are involved in computer network operations, including computer network defense, exploitation, and computer network attack. We reviewed a variety of unclassified and classified documents to understand the organization and challenges the department faces in addressing cyberspace operations.

To evaluate DOD's organization to address cybersecurity threats, we reviewed classified and unclassified documents and interviewed officials from a range of DOD organizations involved in computer network operations. We coordinated our work at the following DOD offices:

Offices within the Office of the Secretary of Defense

- Assistant Secretary of Defense for Homeland Defense and America's Security Affairs
- Assistant Secretary of Defense for Network and Information Integration / Chief Information Officer
- Under Secretary of Defense for Acquisition, Technology and Logistics, Science and Technology
- Under Secretary of Defense for Intelligence
- Under Secretary of Defense for Policy

Joint Staff Directorates

Combatant Commands

- U.S. Strategic Command
 - Joint Functional Component Command–Network Warfare
 - Joint Task Force–Global Network Operations
 - Joint Information Operations Warfare Command
- U.S. Joint Forces Command
- U.S. Special Operations Command
- U.S. Central Command
- U.S. Pacific Command
 - U.S. Pacific Air Forces
 - U.S. Army Pacific Forces
 - U.S. Pacific Fleet
 - U.S. Marine Forces Pacific
- U.S. European Command
 - U.S. Army Europe
 - U.S. Air Force Europe
 - U.S. Navy Europe

	<ul style="list-style-type: none">• U.S. Africa Command• U.S. Northern Command
Department of the Army	<ul style="list-style-type: none">• Army Network Operations Security Center• Army National Guard
Department of the Navy	<ul style="list-style-type: none">• Naval Network Warfare Command• Naval Research Laboratory• Marine Corps Network Operations Security Center
Department of the Air Force	<ul style="list-style-type: none">• Headquarters, Cyberspace Operations• U.S. Space Command• 24th Numbered Air Force (Provisional)• 67th Network Warfare Wing• Air Force Information Operations Center• Air Force National Guard
DOD Agencies	<ul style="list-style-type: none">• National Security Agency• Defense Information Systems Agency• Defense Cyber Crimes Center• Defense Intelligence Agency
Defense Criminal Investigative Organizations	<ul style="list-style-type: none">• U.S. Department of Defense, Office of Inspector General, Defense Criminal Investigative Service• Naval Criminal Investigative Service• Air Force Office of Special Investigations• U.S. Army Criminal Investigation Command
Federal Agencies and Entities	<ul style="list-style-type: none">• National Security Council• Office of the Director of National Intelligence• Department of Homeland Security• Department of Justice, Federal Bureau of Investigation
Nongovernmental Cybersecurity Organizations	<ul style="list-style-type: none">• Sans Institute• Carnegie Mellon CERT CC

We reviewed policies, guidance, and directives involving organizations related to computer network operations. Also, we reviewed documents involving the reorganization and development of new organizations within

the Office of the Secretary of Defense, U.S. Strategic Command, Air Force, and Navy to address cyber threats.

To determine the extent to which DOD has developed an overarching joint doctrine that addresses cyberspace operations across DOD, we reviewed and analyzed current joint doctrine publications, such as Joint Publication 13-3, *Information Operations*, and other publications involving computer network operations for key definitions. Also, we reviewed U.S. Joint Forces Command's analysis of cyber-related joint doctrine and U.S. Strategic Command's current efforts to develop joint doctrine. In addition, we interviewed Joint Staff, U.S. Strategic Command, and U.S. Joint Forces Command officials regarding current department efforts to develop joint doctrine on cyberspace. We compared existing joint doctrine efforts and plans with the guidance in DOD's joint doctrine development process.

To assess the extent to which DOD has assigned command and control responsibilities, we reviewed the 2008 Unified Command Plan, Standing Rules of Engagement and other DOD plans, policies and guidance to determine authorities for functional and geographic combatant commands, military services, and defense agencies. Additionally, we reviewed and identified lessons learned from combatant commands following DOD's response to malware infections during Operation Buckshot Yankee in 2008. In addition, we interviewed service and command officials directly involved with Operation Buckshot Yankee to discuss their challenges. We also reviewed recommendations on command and control from the Institute for Defense Analyses and U.S. Joint Forces Command and met with officials from these organizations to discuss analysis involving this area.

To determine capability gaps involving computer network operations we analyzed the fiscal year 2010 and 2011-2015 Integrated Priority Lists to identify cyberspace capability gaps for the functional and geographic combatant commands.¹ Also we analyzed the National Intelligence

¹An Integrated Priority List is a list of a combatant commander's highest priority requirements, prioritized across service and functional lines, defining shortfalls in key programs that, in the judgment of the combatant commander, adversely affect the capability of the combatant commander's forces to accomplish their assigned mission. The integrated priority list provides the combatant commander's recommendations for programming funds in the planning, programming, and budgeting system process.

Estimate regarding *The Global Cyber Threat to the U.S. Information Infrastructure*, the Central Intelligence Agency's *Cyber Threat Intelligence Highlights*, and prior GAO reports on cybersecurity to determine the depth of cyber threats facing the nation and DOD. We also interviewed various functional and geographic combatant command officials to identify capability gaps and resources needed to address these gaps. In addition, we met with Joint Staff officials to discuss their efforts to address capability gaps listed in the Integrated Priority Lists, including developing studies on manpower shortages and providing funding to computer network defense efforts. We reviewed DOD cyber-related capability assessments and compared them with DOD criteria for capabilities-based assessments as part of DOD's Joint Capabilities Integration and Development System.

We conducted this performance audit from November 2008 through April 2010 in accordance with generally accepted government auditing standards and worked with DOD from November 2010 to July 2011 to prepare an unclassified version of this report for public release. Government auditing standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: DOD Cyber Organizations

The following are examples of Department of Defense (DOD) offices and organizations with cyber-related roles and responsibilities.

Table 5 shows certain cyber-related roles and responsibilities for various offices within the Office of the Secretary of Defense.

Table 5: Office of the Secretary of Defense Cyber-Related Responsibilities and Efforts

Directorate or organization	Description of effort
Assistant Secretary of Defense for Networks and Information Integration / DOD Chief Information Officer	<ul style="list-style-type: none"> Principal staff assistant to the Secretary of Defense on network policies, information technology, network operations, and information assurance. Provides strategic-level guidance and oversight for computer network operations including network operations and information assurance; the responsibilities include (1) developing and maintaining the DOD information assurance program and associated policies, procedures, and standards; (2) providing DOD-wide policy regarding the use of the Internet and Web site administration; and (3) providing policies, oversight, and guidance for all communications and information network programs and initiatives across DOD. Involved extensively in inter-agency cybersecurity efforts of CNCI including Connecting the Centers, Securing the Classified Networks, Cybersecurity Workforce Training, Education, and Workforce Sizing, Research and Development, Supply Chain Risk Management, and Defense Industrial Base Cybersecurity Efforts.
Under Secretary of Defense for Policy	<ul style="list-style-type: none"> Provides strategic level guidance and oversight for computer network operations, information assurance, and information operations.^a Lead integrator of both cyber policy for interagency and international coordination and of the planning and employment of information operation capabilities outside of the intelligence community.
Under Secretary of Defense for Intelligence	<ul style="list-style-type: none"> Principal staff assistant to the Secretary of Defense for information operations. The Office of the Under Secretary of Defense for Intelligence responsibilities include (1) developing and overseeing DOD information operations policy and integration activities; (2) establishing and overseeing specific policies for the integration of computer network operations, including computer network attack; and (3) serving as the DOD lead on information operation issues within the intelligence community.
Under Secretary of Defense for Acquisitions, Technology and Logistics	<ul style="list-style-type: none"> Responsible for incorporating policy and processes into the DOD acquisition process that support the protection of controlled unclassified information within unclassified defense industrial base networks. Also, responsible for developing DOD-wide policy and maintaining oversight of the process to conduct damage assessments after unauthorized access to DOD information from an unclassified defense industrial base network. The office also is a member of the Defense Industrial Base Executive Committee, a committee chartered to improve the protection of controlled unclassified information with the Defense Industrial Base

Source: GAO analysis of DOD data.

Note: Data are from DOD publications and official statements.

^aAccording to Joint Publication 3-13, *Information Operations*, Computer Network Operations are one of the five core capabilities of Information Operations.

Table 6 shows certain cyber-related roles and responsibilities for various Joint Staff offices.

Table 6: Joint Staff Cyber-Related Responsibilities and Efforts

Joint Staff directorate or division	Description of effort
Global Operations (Information Operations and Computer Network Operations), J-39	<ul style="list-style-type: none"> • Focal point for information operations within the Joint Staff. • Provides recommendations and advice to the President, Secretary of Defense, National Security Council, and Homeland Security Council on all aspects of computer network operations. • In coordination with the Office of the Secretary of Defense, the J-39 division oversees the integration of computer network attack into specific military operations.
Information and Cyberspace Policy, J-5	<ul style="list-style-type: none"> • Develops and coordinates policy and strategies that contribute to effective conduct of information and cyberspace operations. • Cyber division is responsible for developing strategy and policy that contribute to military freedom of action in cyberspace; establishing joint cyberspace policies for effective strategic planning; and fostering joint and interagency collaboration regarding cyberspace issues including national cyber initiatives.
Network Operations, J-63	<ul style="list-style-type: none"> • Develops DOD and Joint Staff strategies and positions for cyberspace and network operations. • Recommends and synchronizes cyberspace and network operations guidance in joint doctrine. • Research, reviews, and synchronizes DOD and joint network operations policies in DOD directives, instructions, and Joint Staff policies.
Joint Education and Doctrine, J-7	<ul style="list-style-type: none"> • Coordinates with the military services and combatant commands to integrate computer network attack and information operations doctrine into joint doctrine for military operations

Source: GAO analysis of DOD information.

Note: Data are from DOD Web sites.

Table 7 shows certain cyber-related coordination forums.

Table 7: Cyber-Related Coordination Forums

Name	Description of effort
Cyberspace Integration Group	<ul style="list-style-type: none"> An oversight council that was established to: (1) monitor the implementation plan of the National Military Strategy for Cyberspace Operations; (2) ensure that the implementation plan is coordinated amongst the members and combatant commands; (3) seek consensus on cyberspace policy; (4) present recommendations; and (5) mediate disputes. Co chaired by the Joint Staff and the U.S. Strategic Command and consists of three-star general/flag officers or their representatives and members from the Joint Staff, Office of the Secretary of Defense, U.S. Strategic command, U.S Joint Forces command, military services, Defense Information Systems Agency, National Security Agency, and U.S Special Operations Command.
Cyberspace Integration Team	<ul style="list-style-type: none"> Standing working group, chaired by the Joint Staff J-5 division, that brings DOD cyber stakeholders together for regular meetings at the Pentagon. Chartered to synchronize cyberspace operational, planning, and policy efforts to ensure effective, integrated operations in cyberspace and inform existing Joint Staff process and provide updates to the Chairman of the Joint Chiefs of Staff as required. The team also facilitates the coordination and integration of cyberspace issues associated with the <i>National Military Strategy for Cyberspace Operations</i>. The team was originally established within the Joint Staff to include all Joint Staff directorates, but it expanded to include the military services, the Office of the Secretary of Defense, U.S. Strategic Command, and other DOD agencies.

Source: GAO analysis of DOD information.

Table 8 shows certain cyber-related roles and responsibilities of U.S. Strategic Command.

Table 8: Roles and Responsibilities of U.S. Strategic Command

Name	Roles and responsibilities
U.S. Strategic Command	<ul style="list-style-type: none"> Direct DOD's global information grid operations and defense. Planning against designated cyberspace threats. Coordinate with other combatant commands and appropriate U.S. government agencies for matters related to cyberspace, as directed. Advocating for cyberspace capabilities. Executing cyberspace operations, as directed.

Source: GAO analysis of DOD data.

Note: Data are from the Unified Command Plan, 2008.

Table 9 shows certain cyber-related roles and responsibilities of Combatant Command Theater Network Centers and Theater and Global Network Operation Centers.

Table 9: Roles and Responsibilities of Combatant Command Network Centers

Functional component command	Roles and responsibilities
Theater Network Operations Centers	<ul style="list-style-type: none"> Develop, monitor, and maintain situational awareness for respective portion of geographic combatant commands' global information grid. Combatant commands have control over theater forces and theater networks through these centers.
Theater Network Operations Control Centers	<ul style="list-style-type: none"> Maintain situational awareness of their network assets. Lead, prioritize, and direct theater global information grid assets and resources to ensure they are optimized to support geographic combatant command missions and operations. Lead commands' responses to network operations events and respond to Joint Task Force–Global Network Operations direction when required to correct or mitigate a global network operation issue.
Global Network Operations Control Centers	<ul style="list-style-type: none"> Advise the functional combatant command to ensure that global information grid resources are optimized. Monitor the commands' global information grid assets, determine the operational effect of major degradations and outages, and coordinate responses to affect joint operations.

Source: GAO analysis of DOD information.

Note: Data are from DOD publications.

Table 10 shows the cyber-related roles and responsibilities of services' Network Operations Centers and Computer Emergency/Incident Response Teams

Table 10: Roles and Responsibilities of Service Network Centers

Functional component command	Roles and responsibilities
Service Global Network Operations and Security Centers	<ul style="list-style-type: none"> Provides service-specific network operations reporting and situational awareness for the service's portion of the global information grid. Tactical control of Service Global Network Operations and Security Centers is held by the Joint Task Force–Global Network Operations in response to network events.
Computer Emergency / Incident Response Teams	<ul style="list-style-type: none"> Provides service-specific network operations reporting and situational awareness for the service's portion of the global information grid. In response to network activity determined by the Commander of Joint Task Force–Global Network Operations, the commander can assume tactical control over the services' Computer Emergency / Incident Response Teams.

Source: GAO analysis of DOD information.

Note: Data are from DOD report.

Table 11 shows the military services' current cyber organization in January 2009.

Table 11: Cyber Organization of the Military Services as of January 2009

Military service	Organization	Roles and responsibilities
U.S. Army	Army Space Missile Defense Command / Army Force Strategic Command	<ul style="list-style-type: none"> • Planning, coordinating, integrating, and providing oversight to the Army's computer network operations in support of U.S. Strategic Command. • Operating, managing, and defending the network at the enterprise-level infrastructure, with support from the Army's Intelligence and Security Command directed by the Network Enterprise Technology Command / 9th Army Signal Command.
U.S. Navy	Naval Network Warfare Command	<ul style="list-style-type: none"> • Responsibilities include all aspects of information operations, including computer network operations and information assurance, intelligence, networks, and space. • The Navy is currently in the process of transforming its cyber organization and has recently stood up the 10th Fleet, Navy Fleet Cyber Command.
U.S. Marine Corps	Marine Corps Network Operations and Security Center Command	<ul style="list-style-type: none"> • Provides direct support to the geographic combatant commands and Marine forces for theater network operations issues and in its entirety fulfills its direct support responsibilities. • Assigned operational control as a component to the Joint Task Force–Global Network Operations.
U.S. Air Force	24th Air Force, under the Air Force Space Command	<ul style="list-style-type: none"> • Plans and conducts cyberspace operations in support of combatant commands and maintains and defends the Air Force Enterprise Network Global Information Grid. • The Air Force designed their Network Operations and Security Center around their major commands placing the centers in each theater.

Source: GAO analysis of DOD information.

Table 12 shows some of the cyber-related roles and responsibilities of the intelligence agencies.

Table 12: Roles and Responsibilities of Intelligence Agencies

Intelligence agency	Roles and responsibilities
National Security Agency	<ul style="list-style-type: none"> • Responsible for developing, implementing, and overseeing an information assurance program that provides layered protection of DOD cryptologic sensitive compartmented information systems. • Office of Information Operations and Information Warfare support center provides offensive cyber operations, related military targeting support, and intelligence gain/loss assessments. • Director of the National Security Agency serves as executive secretary for DOD and intelligence community deconfliction.

Intelligence agency	Roles and responsibilities
Defense Intelligence Agency	<ul style="list-style-type: none"> Responsible for developing, implementing, and overseeing an information assurance program for protection of the DOD non-cryptologic sensitive compartmented information systems. Provides offensive cyber operations-related military targeting support, political/military assessment, and battle damage assessment of system functional capabilities.
Office of the Director for National Intelligence	<ul style="list-style-type: none"> Serves as the intelligence community focal point for offensive cyber operations strategic planning, policy coordination, and interagency coordination for implementing National Security Presidential Directive 38.

Source: GAO analysis of DOD data.

Table 13 shows certain cyber-related roles and responsibilities of defense criminal investigative–related organizations.

Table 13: Roles and Responsibilities of Defense Criminal Investigative–Related Organizations

Defense criminal investigative organization	Roles and responsibilities
U.S. Naval Criminal Investigative Service	<ul style="list-style-type: none"> Maintains and operates a worldwide federal law enforcement organization to fulfill the investigative and counterintelligence needs of the U.S. Navy and the U.S. Marine Corps. Cyber department prevents terrorism, protects secrets, reduces major crimes and executes advanced cyber technologies and methodologies to process, identify, and present electronic data of intelligence or evidentiary value.
Air Force Office of Special Investigations	<ul style="list-style-type: none"> Provides cyber-related criminal and counterintelligence investigative services to commanders throughout the Air Force. Identifies, investigates, and neutralizes criminal, terrorist, and espionage threats to personnel and resources of the Air Force and Department of Defense.
Defense Criminal Investigative Service	<ul style="list-style-type: none"> Criminal investigative arm of the Department of Defense Inspector General. Investigating matters relating to terrorism, preventing the illegal transfer of sensitive defense technology, stopping cyber crime and computer intrusions, and investigating cases of fraud, bribery, and corruption.
Army Criminal Investigation Command and Army Counterintelligence	<ul style="list-style-type: none"> Army Criminal Investigation Command investigates and prosecutes cyber-related criminal cases. Army Counterintelligence investigates cyber-related counterintelligence cases. The two work closely together to investigate cyber-related cases for the Army.
DOD Cyber Crime Center	<ul style="list-style-type: none"> Provides criminal, counterintelligence, counterterrorism, and fraud-related computer forensics support to the defense criminal investigative organizations. Delivers cyber technical training; digital evidence processing and electronic media analysis for criminal law enforcement and DOD counterintelligence investigations and activities. Performs investigations and provides forensic training to DOD members to ensure that information systems are secure from unauthorized use.

Defense criminal investigative organization

Roles and responsibilities

Defense Industrial Base Collaborative Information Sharing Environment

- Office of the Secretary of Defense–initiated effort to facilitate DOD coordination of threat information-sharing and measures enabling the protection of unclassified DOD information transiting or residing on defense industrial base information systems and networks.
- Run by the DOD Cyber Crime Center, and 29 private-sector defense industrial base partners that have voluntarily agreed to share information through this program as of March 2009.
- The 29 private-sector defense industrial base partners are responsible for approximately 90 percent of the information across the defense industrial base.

Source: GAO analysis of DOD information

Note: Data are from DOD publications and Web sites.

Policy Review for the Office of the Under Secretary of Defense for Policy

The Secretary of Defense directed the office to lead a review of policy and strategy to develop a comprehensive approach to DOD cyberspace operations. As a result of this review and a separate review of DOD cyberspace policy conducted under the *National Military Strategy for Cyberspace Operations Implementation Plan*, the Office of the Under Secretary of Defense for Policy found that DOD required new and updated cyberspace policies to guide the integration of cyberspace, and that the existing policies were too focused on the individual pieces of cyberspace operations.

Table 14 shows how the military services are supporting or plan to support the U.S. Cyber Command.

Table 14: Current or Proposed Cyber Organization of the Military Services

Military service	Organization	Roles and responsibilities
U.S. Army	Army Forces Cyberspace Command	<ul style="list-style-type: none"> • Its anticipated to plan, coordinate, integrate, synchronize, and defend the Army’s portion of DOD network and conduct, when directed, offensive operations in cyberspace.
U.S. Navy	Fleet Cyber Command, 10th fleet	<ul style="list-style-type: none"> • Its mission is to serve as the central operational authority for networks, intelligence, information operations, cyber, electronic warfare, and space and to operate a secure and interoperable naval network. • The Fleet Command will also have operational control of the Navy cyber, network operations, and information operations forces. • The Naval Network Warfare Command will become subordinate to the Fleet Cyber Command and will execute only network and space operations.
U.S. Marine Corps	Marine Forces Cyber	<ul style="list-style-type: none"> • Its mission is anticipated to support U.S. Cyber Command in all defensive and offensive mission areas. • The Commander of Marine Forces Strategic Command is also anticipated to serve as the Commander of Marine Forces Cyber.

Appendix II: DOD Cyber Organizations

Military service	Organization	Roles and responsibilities
U.S. Air Force	24th Air Force	<ul style="list-style-type: none">• It is designated as Air Forces Cyber in support of the U.S. Cyber Command.• Its mission is to establish, operate, defend, exploit, and attack in cyberspace.

Source: GAO analysis of DOD information.

Note: Data are from DOD briefings and publications.

Appendix III: Cyberspace Defensive Measures and Mechanisms Used by DOD

The Department of Defense (DOD) defines computer network defense as actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. Computer network defense employs information assurance capabilities to respond to unauthorized activity within DOD information systems and computer networks in response to a computer network defense alert or threat information.

Currently, DOD's cyberspace defensive measures include Intrusion Detection Systems that alert network operators to the signatures of an incoming attack or can kill the network traffic. Strong firewall settings reduce the exposure to the outside world on the NIPR Network as well as block incoming traffic from origins known to launch attacks. Traffic, both inbound and outbound, in a symmetric network configuration, can be examined or prevented, causing most trivial attacks to be stopped at the NIPR Network borders.

Several metrics are used to measure information assurance performance. These include documenting the correct certification and accreditation documentation and compliance with DOD directives, reporting this information as a part of the Federal Information Systems Management Act, vulnerability scanning, red and blue team testing, Defense Information Systems Agency evaluations performed on various networks, and other efforts.

Below are several examples of policies, programs, and tools that DOD uses to protect its networks.

Computer Network Defense Service Providers

DOD Directive O-8530.1, and its supporting document DOD Instruction O-8530.2, directed the heads of all DOD components to establish component-level computer network defense services to coordinate and direct all componentwide computer network defense and ensure certification and accreditation in accordance with established DOD requirements and procedures.¹ Computer network defense service is provided or subscribed to by owners of DOD information systems or

¹DOD, Directive O-8530.1, *Computer Network Defense* (Washington D.C., January 2001) and DOD Instruction O-8530.2, *Support to Computer Network Defense* (Washington D.C., March 2001).

computer networks, or both, in order to maintain and provide computer network defense situational awareness, implement computer network defense protect measures, monitor and analyze in order to detect unauthorized activity, and implement computer network defense operational direction. DOD Directive O-8530.1 also required that all component information systems and computer networks be assigned to a certified computer network defense service provider. Computer network defense service providers are those organizations responsible for delivering protection, detection, and response services to its users. Computer network defense service providers are commonly a Computer Emergency or Incident Response Team and may be associated with a Network Operations and Security Center. The goal for the program is to improve the security posture of DOD information systems and networks by ensuring that a baseline set of services are provided by computer network defense service providers. Under the oversight of the Assistant Secretary of Defense for Networks and Information Integration and U.S. Strategic Command, the Defense Information Systems Agency conducts a certification program of the computer network defense service providers to ensure they are providing that critical baseline set of services.

Defense Information Assurance Certification and Accreditation Process Training

The Defense Information Assurance Certification and Accreditation Process was implemented by the DOD Chief Information Officer in DOD Instruction 8510.01 on November 28, 2007.² According to DOD, the Defense Information Assurance Certification and Accreditation Process is the standard DOD process for identifying, implementing, validating, certifying, and managing information assurance capabilities and services, expressed as information assurance controls, and authorizing the operation of DOD information systems, in accordance with Title III of the E-Government Act, the Federal Information Security Management Act, DODD 8500.1, DODI 8500.2, and other statutory and regulatory requirements.³

²DOD, Instruction 8510.01, *DOD Information Assurance Certification and Accreditation Process* (Washington D.C., November 2007).

³DOD, Directive 8500.1, *Information Assurance* (Washington D.C., October 2002) and DOD, Instruction 8500.2, *Information Assurance Implementation* (Washington D.C., February 2003).

Federal Information Security Management Act

The Federal Information Security Management Act of 2002 requires agencies to develop and implement an information security program, evaluation processes, and annual reporting.⁴ The act requires mandated annual reports by federal agencies and the Office of Management and Budget. The act also includes a requirement for independent annual evaluations of the agencies' information security programs and practices by the agencies' inspectors general or independent external auditors.

Host-Based Security Systems

Host-Based Security Systems are a suite of commercial-off-the-shelf software that provides a framework and point products to protect against cyber threats both at the network and host levels, and provide system baselining to support the Information Operations Condition process.⁵ The system includes, but is not limited to, host firewall, host intrusion detection, host intrusion prevention, system compliance profiling, rogue system detection, application blocking, and Information Operations Condition baselining. DOD expects to provide network administrators and security personnel with mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DOD networks and information systems. The deployment of Host-Based Security Systems was initially ordered by Joint Task Force-Global Network Operations in October 2007, with deployment on unclassified systems to be completed no later than June 2008. Deployment of Host-Based Security Systems to classified systems was to begin in January 2008. According to U.S. Strategic Command, as of February 2010, DOD NIPR and SIPR networks were still in the process of implementing Host-Based Security Systems, with 67 percent and 48 percent respectively implemented.

⁴The Federal Information Security Management Act was enacted as Title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002) (codified at 44 U.S.C. §§ 3541-3549).

⁵INFOCON, or Information Operations Condition, is a system that provides a framework within which the Commander of U.S. Strategic Command, regional commanders, service chiefs, base/post/camp/station/vessel commanders, or agency directors can increase the measurable readiness of their networks to match operational priorities. U.S. Strategic Command, Directive SD 527-1, *Department of Defense (DOD) Information Operations Condition (INFOCON) System Procedures*, (Jan. 27, 2006).

**Information Assurance
Vulnerability Management
Program**

The Information Assurance Vulnerability Management Program provides positive control of vulnerability notification, corresponding corrective action, and Information Assurance Vulnerability Alert status visibility for DOD network assets. It focuses on the status of DOD networks to mitigate or eliminate known vulnerabilities. Joint Task Force–Global Network Operations is responsible for monitoring relevant sources of information to discover security conditions that may require Information Assurance Vulnerability Management vulnerability notification and assess risk and potential operational effect associated with software vulnerabilities. Once a vulnerability is evaluated and warrants notification, Joint Task Force–Global Network Operations will publish an Information Assurance Vulnerability Management vulnerability notification and amplifying information as one of three products depending on risk level of the vulnerability: Information Assurance Vulnerability Alert (critical risk), Information Assurance Vulnerability Bulletin (medium risk), Technical Advisory (low risk). Response to Alerts is mandatory and combatant commands, military services, and defense agencies are required to implement directives, and report back to Joint Task Force–Global Network Operations on their Information Assurance Vulnerability Alert compliance.

**Command Cyber
Readiness Inspection**

These inspections, formerly known as the Enhanced Compliance Validation visits, are conducted by the Defense Information Systems Agency at the direction of U.S. Strategic Command in order to provide an assessment of information assurance and compliance to DOD policies and configuration requirements of all combatant commands, military services, and DOD agencies. The Defense Information Systems Agency also uses these inspections to provide DOD component and local leadership with actionable recommendations for improving information assurance readiness. DOD officials considered these visits as risk assessments.

Operational Inspections

Inspection teams provide penetration testing and security audits for client agencies, combatant commands, installations, and military services. The inspection teams use a holistic approach that evaluates more than computer hardware and software—such as personnel procedures and policies, and physical security of equipment and locations.

Network Scans

According to Defense Information Systems Agency officials, the Defense Information Systems Agency and Joint Task Force–Global Network Operations scan DOD networks. Combatant commands, military services,

and defense agencies are also responsible for scanning the local systems that they administer. The Defense Information Systems Agency scans systems prior to their connection to DOD networks and at regularly scheduled intervals thereafter. Additionally, Joint Task Force–Global Network Operations has directed all combatant commands, military services, and defense agencies to scan their networked devices on a regular basis.

**Joint Task Force–Global
Network Operations
Scorecard**

Joint Task Force–Global Network Operations has developed its NetOps Scorecard as a process for displaying NetOps compliance and readiness status for the entire DOD community. This quarterly review has been in effect for the military services since August 2007, and was expanded to cover all combatant commands, military services, and DOD agencies in February 2009. The Scorecard measures compliance to NetOps directives (such as communications tasking orders, Information Operations Conditions, and fragmentary orders), authority to operate, Information Assurance Vulnerability Alert compliance, and the status of inspections.

**U.S. European Command
Cyber Defense Playbook**

U.S. European Command has developed its own Cyber Defense Playbook intended to standardize theater policy, tactics, and procedures related to computer network defense efforts and improve command and control relationships to ensure and maintain cyber/network readiness and coordinated responses to computer network defense events. The Playbook was developed by a working group from across the theater with participation from U.S. European Command, U.S. Army Europe, U.S. Air Force Europe, Special Operations Command Europe, U.S. Navy Europe, and the Defense Information Systems Agency. It incorporates information and best practices from the agencies listed above as well as from the Joint Functional Component Command for Network Warfare and Joint Staff guidance. It includes baseline computer network defense triggers, reporting and response timelines, checklists, tactics, techniques, and procedures for computer network defense related events, and basic computer network defense reference materials. The Playbook also includes contingency options for personnel to use should their recommended computer network defense tools be unavailable.

Defense Industrial Base
Collaborative Information
Sharing Environment

According to officials from the DOD Cyber Crime Center, the Defense Industrial Base Collaborative Information Sharing Environment is an Office of the Secretary of Defense–initiated effort to generate more transparency about and share network security information among DOD’s private sector contractors. The Defense Industrial Base Collaborative Information Sharing Environment is run by the DOD Cyber Crime Center, and 28 Defense Industrial Base partners have voluntarily agreed to share information through the program as of March 2009. The 28 Defense Industrial Base partners are all major contractors and are responsible for approximately 90 percent of the information across the Defense Industrial Base. The information shared in Defense Industrial Base Collaborative Information Sharing Environment is anonymous because the Defense Industrial Base partners are concerned about public disclosure. They feel that if their shareholders and competitors learn that a Defense Industrial Base partner’s networks have been attacked, it could affect earning and the ability to win contracts in the future.

National Cyber Range

The Defense Advanced Research Projects Agency is in the process of developing a National Cyber Range that will provide a test bed to produce qualitative and quantitative assessments of the security of various cyber technologies and scenarios. This effort is expected to provide a safe, instrumented environment for national cyber security research organizations to test the security of information systems. Several private, commercial, and academic institutions will develop the initial phase of the National Cyber Range. At the conclusion of the initial phase, the Defense Advanced Research Projects Agency will make decisions regarding future plans, which notionally could include a second phase with a critical design review, and a third phase to develop the full-scale National Cyber Range and start conducting tests.

DOD Security Technical
Implementation Guides
(STIG)

According to DOD officials, DOD mandates specific configuration settings for all prevalent technologies in the Global Information Grid through the use of Security Technical Implementation Guides and associated checklists. These Security Technical Implementation Guides are developed by the Defense Information Systems Agency in full collaboration with military services, agencies and selected combatant commands. According to DOD officials, the Security Technical Implementation Guides are updated periodically keeping pace with documented emerging threats and changes to technology. These Security Technical Implementation Guides are a basis for system

administrators to securely maintain their systems and for certifiers and reviewers to evaluate those systems.

Appendix IV: Audit Community Work in Information Security

In prior reports, we and various agency inspector general offices have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program shortfalls.⁶⁹ For example, we recommended that federal agencies correct specific information-security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring, physical security, configuration management, segregation of duties, and continuity of operations planning. We have also recommended that agencies fully implement comprehensive, agencywide information-security programs by correcting weaknesses in risk assessments, information-security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions.

In the past, we have also reviewed the Department of Defense's (DOD) information-security weaknesses in various reports. For example, in 1991, we reported on foreign hackers penetrating DOD computer systems between April 1990 and May 1991, as a result of inadequate attention to computer security, such as password management and the lack of technical expertise on the part of some system administrators.⁷⁰ In May 1996, we reported that unknown and unauthorized individuals were increasingly attacking and gaining access to highly sensitive unclassified information on DOD's computer systems.⁷¹ We reported that external attacks on DOD computer systems were a serious and growing threat. According to DOD officials, attackers had stolen, modified, and destroyed both data and software. They had installed "back doors" that circumvented normal system protection and allowed attackers

⁶⁹GAO, *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses*, [GAO-09-546](#) (Washington, D.C.: July 17, 2009). A sample of reports on information security include: GAO, *Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems*, [GAO-05-231](#) (Washington, D.C.: May 13, 2005); GAO, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, [GAO-08-571T](#) (Washington, D.C.: Mar. 12, 2008); GAO, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, [GAO-09-432T](#) (Washington, D.C.: Mar. 10, 2009); and GAO, *Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk*, [GAO-09-661T](#) (Washington, D.C.: May 5, 2009).

⁷⁰GAO, *Computer Security: Hackers Penetrate DOD Computer Systems*, [GAO/T-IMTEC-92-5](#) (Washington, D.C.: Nov. 20, 1991).

⁷¹GAO, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, [GAO/AIMD-96-84](#) (Washington, D.C.: May 22, 1996).

unauthorized future access. They had shut down and crashed entire systems and networks. In September 1996, we issued a report, based on detailed analyses and testing of general computer controls, that identified pervasive vulnerabilities in DOD information systems.⁷² We had found that authorized users could also exploit the same vulnerabilities that made external attacks possible to commit fraud or other improper or malicious acts. In fact, knowledgeable insiders with malicious intentions could pose a more serious threat than outsiders, since they could be more aware of system weaknesses and how to disguise inappropriate actions. Our report highlighted the lack of a comprehensive information security program and made numerous recommendations for corrective actions. In August 1999, we reported that DOD had made limited progress in correcting the general control weaknesses we reported in 1996.⁷³ We also found that serious weaknesses in DOD information security continued to provide both hackers and hundreds of thousands of authorized users opportunities to modify, steal, inappropriately disclose, and destroy sensitive DOD data. As a result, numerous defense functions, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll, have already been adversely affected by system attacks or fraud. In 2003, we reported that DOD faced many risks in its use of globally networked computer systems to perform operational missions—such as identifying and tracking enemy targets—and daily management functions, such as paying soldiers and managing supplies. Weaknesses in these systems, if present, could give hackers and other unauthorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive military data.

In addition, the Department of Defense Inspector General has completed annual reviews under the Federal Information Security Management Act involving a wide range of information assurance weaknesses that persist throughout DOD systems and networks.⁷⁴ These reports have compiled information assurance vulnerabilities based on reports from Army Audit

⁷²GAO, *DOD General Computer Controls: Critical Need to Greatly Strengthen Computer Security Program*, [GAO/AIMD-96-144](#) (Washington, D.C.: Sept. 30, 1996).

⁷³GAO, *DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk*, [GAO/AIMD-99-107](#) (Washington, D.C.: Aug. 26, 1999).

⁷⁴United States Department of Defense Inspector General Report No. D-2009-110, *Summary of Information Assurance Weakness Found in Audit Reports Issued from August 1, 2008 Through July 31, 2009* (Arlington, Va., Sept. 28, 2009).

Agency, Naval Audit Service, Air Force Audit Agency, and GAO since 1991. From August 1, 2008, to July 31, 2009, the most frequently cited weaknesses were in the following information assurance areas: security policies and procedures/management oversight; access controls; configuration management; and plans of action and milestones to identify, assess, prioritize, and monitor the progress of corrective efforts for security weaknesses found in programs and systems. According to the DOD Inspector General, persistent weaknesses in information-security policies and practices continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support operations, assets, and personnel. The report also noted that without effective management oversight, DOD cannot be assured that systems are accurately reported and maintained, information systems contain reliable data, and personnel are properly trained in security policies and procedures.

Appendix V: Comments from the Department of Defense



GLOBAL STRATEGIC
AFFAIRS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
2900 DEFENSE PENTAGON
WASHINGTON, DC 20301-2900

Ms. Davi M. D'Agostino
Director, Defense Capabilities & Management,
General Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. D'Agostino:

Thank you for the opportunity to comment on the GAO Draft Report, [REDACTED], "DEFENSE MANAGEMENT: DoD Faces Challenges in its Cyber Efforts," dated March 15, 2010 (GAO Code 351273). The Department concurs with the four GAO recommendations identified in the draft report and is actively pursuing the necessary actions to: complete an assessment of joint doctrine; promulgate clear guidance for command and control relationships; develop a comprehensive capabilities-based assessment of the department-wide cyberspace-related mission; and, develop an implementation plan and funding strategy for addressing gaps resulting from the assessment (Atch).

If you have questions, please do not hesitate to contact my point of contact, Mr. Michael Cooksey at (703) 418-6933, Michael.Cooksey@osd.mil.

Sincerely,

Brig Gen Jay G. Santee, USAF
Principal Director, Cyber and Space Policy

Enclosure:
As stated



UNCLASSIFIED

GAO DRAFT REPORT – DATED March 15, 2010
GAO CODE 351273/ [REDACTED]

“DEFENSE MANAGEMENT: DoD Faces Challenges In Its Cyber Efforts”

DEPARTMENT OF DEFENSE COMMENTS
TO THE RECOMMENDATIONS

(U) **GAO RECOMMENDATION 1:** The GAO recommends that the Secretary of Defense direct the Chairman of the Joint Chiefs of Staff in consultation with the Under Secretary of Defense for Policy (USD(P)) and the U.S. Strategic Command (USSTRATCOM) to establish a timeframe for: (1) deciding whether or not to proceed with a dedicated joint doctrine publication on cyberspace operations; and (2) updating the existing body of joint doctrine to include complete cyberspace related definitions.

(U) **DOD RESPONSE:** The Department concurs with this recommendation. As part of implementing the National Military Strategy for Cyberspace Operations, an assessment of joint doctrine has commenced and is expected to be completed by the end of FY11. This joint doctrine process will also include related lexicon/definitions which will be synthesized with the interagency work on cyber lexicon. Additionally, the Department has completed a framework for a new “*National Defense Strategy for Cyberspace Operations*”. This draft strategy takes into consideration the standup of USCYBERCOM, and the results of the 2010 Quadrennial Defense Review, 2010 National Security Strategy, and the 2008 National Defense Strategy. The National Defense Strategy for Cyberspace Operations will address changes in threat conditions since the National Military Strategy for Cyberspace Operations was published in 2006. Within Defense, this year’s Quadrennial Defense Review Report detailed the “*need for improved capabilities to counter threats in cyberspace*” and asserted that “*DOD must be prepared not only to protect the perimeter of our defense and military networks, but also to defend those networks by actively engaging adversaries known to be causing harm*”. This framework has already been used to inform preparations of the Defense Planning and Programming Guidance (DPPG), the Guidance for the Employment of the Force (GEF), and the Front End Analysis (FEA).

(U) **GAO RECOMMENDATION 2:** The GAO recommends that the Secretary of Defense direct the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense for Intelligence (USD(I)) and the Joint Staff to clarify DoD guidance on command and control relationships between the U.S. Strategic Command (USSTRATCOM), the Services, and the geographical combatant commands regarding cyberspace operations and establish a timeframe for issuing the clarified guidance.

UNCLASSIFIED

1

UNCLASSIFIED

GAO DRAFT REPORT – DATED March 15, 2010
GAO CODE 351273/ [REDACTED]

“DEFENSE MANAGEMENT: DoD Faces Challenges In Its Cyber Efforts”

DEPARTMENT OF DEFENSE COMMENTS
TO THE RECOMMENDATIONS

(U) **DOD RESPONSE:** The Department concurs with this recommendation and considers this complete. The Secretary of Defense, through the 23 June 2009 Memorandum as well as the Unified Command Plan (UCP), has promulgated clear guidance for command and control relationships between the U.S. Strategic Command (USSTRATCOM), the Services, and the geographic combatant commands regarding cyberspace operations.

(U) **GAO RECOMMENDATION 3:** The GAO recommends that the Secretary of Defense direct the appropriate Office of the Secretary of Defense officials, in coordination with the Secretaries of the military departments, and the Joint Chiefs of Staff (JCS) to develop a comprehensive capabilities-based assessment of the department-wide cyberspace-related mission and a timeframe for its completion.

(U) **DOD RESPONSE:** The Department concurs with this recommendation. The Secretary of Defense selected cyber defense as one of eight issues for a Front End Assessments for the FY 2012-16 program-budget cycle with a common focus on identifying operational risk and mitigation of that risk, and the need for management and/or authorities adjustments to improve efficiency or performance.

(U) **GAO RECOMMENDATION 4:** The GAO recommends that the Secretary of Defense direct the appropriate Office of the Secretary of Defense officials, in coordination with the Secretaries of the military departments, and the Joint Chiefs of Staff (JCS) to develop an implementation plan and funding strategy for addressing any gaps resulting from the assessment that require new capability development or modifications to existing programs.

(U) **DOD RESPONSE:** The Department concurs with this recommendation. The Front End Assessment as well as the development of the National Defense Strategy for Cyberspace Operations will inform the Department on the gaps and the requisite mitigation strategy required.

UNCLASSIFIED

2

Appendix VI: GAO Contacts and Staff Acknowledgments

GAO Contacts

Davi D'Agostino, (202) 512-5431 or dagostinod@gao.gov

Greg Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Lorelei St. James, Joseph Kirschbaum, Nelsie Alcoser, Neil Feldman, David Holt, Jamilah Moon, Grace Coleman, Joanne Landesman, and Gregory Marchand made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

