

GAO

Report to Senate Committee on
Homeland Security and Governmental
Affairs

October 2012

HOMELAND DEFENSE

DOD Needs to Address Gaps in Homeland Defense and Civil Support Guidance



Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE OCT 2012		2. REPORT TYPE		3. DATES COVERED 00-00-2012 to 00-00-2012	
4. TITLE AND SUBTITLE Homeland Defense: DOD Needs to Address Gaps in Homeland Defense and Civil Support Guidance				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Government Accountability Office, 441 G Street NW, Washington, DC, 20548				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 42	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



Highlights of [GAO-13-128](#), a report to Senate Committee on Homeland Security and Governmental Affairs

Why GAO Did This Study

Defending U.S. territory and citizens is the highest priority of DOD, and providing defense support of civil authorities is one of the department's primary missions. DOD is the federal agency with lead responsibility for homeland defense, whereas for civil support missions DOD provides assistance to the lead civilian federal agency, such as DHS, when requested by the agency or directed by the President for major disasters, emergencies, and special events. This report examines the extent to which DOD has issued current guidance, including doctrine, policy, and strategy, for its homeland defense and civil support missions. To do this, GAO analyzed DOD homeland defense and civil support guidance and plans and met with select DOD and National Guard officials.

What GAO Recommends

This report makes several recommendations to address gaps in DOD's guidance for homeland defense and civil support, including for DOD to assess and, when needed, update its primary strategy; develop implementation guidance on the dual-status commander construct; and align guidance on preparing for and responding to domestic cyber incidents with national-level guidance to include roles and responsibilities. In comments on the draft report, DOD concurred or partially concurred with these recommendations. DOD concurred with our strategy and dual-status commander recommendations and partially concurred with our domestic cyber recommendation. DHS concurred with our domestic cyber recommendation.

View [GAO-13-128](#). For more information, contact Brian Lepore at (202) 512-4523 or leporeb@gao.gov.

October 2012

HOMELAND DEFENSE

DOD Needs to Address Gaps in Homeland Defense and Civil Support Guidance

What GAO Found

The Department of Defense (DOD) protects the U.S. homeland through two distinct but interrelated missions: (1) homeland defense, which defends against threats such as terrorism, weapons of mass destruction, and cyber incidents; and (2) civil support, which involves supporting other federal agencies in responding to major domestic disasters, emergencies, and special events. DOD has issued and updated several key pieces of doctrine, policy, and strategy for homeland defense and civil support, but it has not updated its primary Strategy for Homeland Defense and Civil Support since it was initially issued in 2005 and does not have a process—similar to that for its joint publications and directives—to do so. The Joint Staff determined in August 2010 that joint publications on homeland defense needed a complete revision. The joint publication on civil support is also being revised. U.S. Northern Command, the combatant command responsible for homeland defense, is revising these publications to reflect changes in national and department priorities and to incorporate lessons learned from exercises and events such as Hurricane Katrina. Still, such key national- and department-level strategies and significant events are not reflected in DOD's strategy, in part because the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs does not have a process for periodically assessing the currency of its homeland defense and civil support strategy and ensuring that needed updates are completed in a timely manner. Reliance on an outdated strategy could hinder DOD's ability to effectively plan for and respond to major disasters and emergencies.

DOD issued some guidance on the dual-status commander construct—through which, during a civil support incident or special event, a single military officer has authority over both National Guard and active-duty military personnel, serving as a link between state and federal forces. Nevertheless, gaps in guidance remain because DOD has not yet developed comprehensive policies and procedures regarding the use and availability of dual-status commanders, including specific criteria and conditions for when and how a state governor and the Secretary of Defense would mutually appoint a commander. For example, DOD has not developed guidance for the use of dual-status commanders for incidents affecting multiple states and territories, and it does not have a process to determine the appropriate mix of National Guard and active duty federal officers to meet DOD's anticipated needs. As a result, DOD's ability to adequately prepare for and effectively use dual-status commanders for a range of civil support events, including those affecting multiple states, may be hindered.

While a 2010 DOD Directive, a 2007 joint publication, and an agreement with the Department of Homeland Security (DHS) provide some details on how DOD should respond to requests for civil support in the event of a domestic cyber incident, they do not address some aspects of how DOD will provide support during a response. First, DOD has not clarified its roles and responsibilities, and chartering directives for DOD's Offices of the Assistant Secretaries for Global Strategic Affairs and for Homeland Defense and Americas' Security Affairs outline conflicting and overlapping roles and responsibilities. Second, DOD has not ensured that its civil support guidance is aligned with national plans and preparations for domestic cyber incidents. Consequently, it is unclear whether DOD will be adequately prepared to support DHS during a cyber incident.

Contents

Letter		1
	Background	3
	Some DOD Homeland Defense and Civil Support Mission Guidance Is Outdated or Incomplete, and No Routine Process Exists to Ensure Regular Updating	9
	Conclusions	21
	Recommendations for Executive Action	21
	Agency Comments and Our Evaluation	22

Appendix I	Scope and Methodology	25
------------	-----------------------	----

Appendix II	Comments from the Department of Defense	28
-------------	---	----

Appendix III	Comments from the Department of Homeland Security	32
--------------	---	----

Appendix IV	GAO Contact and Staff Acknowledgments	34
-------------	---------------------------------------	----

Related GAO Products		35
----------------------	--	----

Tables		
	Table 1: DOD Organizations that have Key Roles and Responsibilities in Homeland Defense and Civil Support	7
	Table 2: Some Key Department and National Level Policies and Guidance that DOD Uses for its Homeland Defense and Civil Support Missions	10
	Table 3: Offices We Met with During our Review	26

Figures		
	Figure 1: Examples of DOD's Homeland Defense and Civil Support Missions	4

Figure 2: Relevant Areas of Responsibility for U.S. Northern Command and U.S. Pacific Command	6
Figure 3: Number of Trained and Certified Dual-Status Commanders in the 54 U.S. States and Territories, as of June 2012	17

Abbreviations

DOD Department of Defense
DHS Department of Homeland Security

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

October 24, 2012

The Honorable Joseph Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate

Defending U.S. territory and citizens is the highest priority of the Department of Defense (DOD), and providing appropriate defense support of civil authorities is one of the department's primary missions.¹ DOD protects the homeland through two distinct but interrelated missions: homeland defense—which it conducts through air, land, maritime, space, and cyber operations, with other agencies supporting DOD's efforts—and civil support²—which involves supporting other agencies in responding to major disasters and emergencies,³ significant domestic cyber incidents, and special events such as presidential inaugurations and major international summits held in the United States. A significant cyber incident could include a deliberate act by an organization or individual to

¹Department of Defense *Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense* (Washington, D.C.: January, 2012).

²For the purposes of this report, civil support refers to defense support of civil authorities, which is DOD's mission to provide support through the federal military force, National Guard, and other resources in response to requests for assistance from civil authorities for special events, domestic emergencies, designated law enforcement support, and other domestic activities.

³42 U.S.C. § 5122 defines major disasters and emergencies. A major disaster is any natural catastrophe (including any hurricane, tornado, storm, high water, wind-driven water, tidal wave, tsunami, earthquake, volcanic eruption, landslide, mudslide, snowstorm, or drought), or, regardless of cause, any fire, flood, or explosion, in any part of the United States, which in the determination of the President causes damage of sufficient severity and magnitude to warrant major disaster assistance to supplement the efforts and available resources of states, local governments, and disaster relief organizations in alleviating the damage, loss, hardship, or suffering caused thereby. An emergency is an occasion or instance for which, in the determination of the President, federal assistance is needed to supplement state and local efforts and capabilities to save lives and to protect property and public health and safety, or to lessen or avert the threat of a catastrophe in any part of the United States.

impede computer networks and infrastructure within the United States that threatens lives, property, the economy, or national security.

DOD serves as the lead federal agency for homeland defense. For DOD's civil support mission, DOD provides assistance to the lead civilian federal agency, such as the Department of Homeland Security (DHS), when requested by the agency and when approved by the Secretary of Defense or when directed by the President. DOD supports numerous civil support missions, such as the recent response to wildfires in Colorado. However, since DOD only supports other agencies in these types of missions, DOD generally does not train, or equip specifically to satisfy civil support mission requirements except for key specialized missions in chemical, biological, radiological, and nuclear response. In responding to major disasters and emergencies, DOD can use a dual-status commander—a military officer who has authority over both active duty federal and state National Guard forces and who serves as an intermediate link between state and federal chains of command when employed simultaneously. A dual-status commander requires specialized training to promote a unity of effort between federal and state forces to facilitate a rapid response to save lives, prevent human suffering, and protect property in the United States.

To date, we have issued several products on the progress DOD has made to address issues related to homeland defense and civil support since U.S. Northern Command was established in October 2002, after the September 11, 2001 terrorist attacks. Among other things, these reports have focused on issues and made recommendations involving coordination within DOD, including between U.S. Northern Command and U.S. Pacific Command and with other federal agencies in preparing for and responding to homeland defense and civil support missions; conducting staffing and needs assessments for civil support; DOD's management of its aerospace control alert mission⁴ and chemical, biological, radiological, and nuclear incidents; U.S. Northern Command's homeland defense and civil support exercise program; and U.S. Northern Command's homeland defense and civil support guidance development and planning efforts. These reports are listed in the Related GAO Products section at the end of this report.

⁴This mission was formerly known as air sovereignty alert.

You asked us to examine DOD's efforts to develop doctrine and assess capability requirements for homeland defense and civil support. This report is a public version of a sensitive report, issued in September 2012 and examines the extent to which DOD has issued current guidance, including doctrine, policy, and strategy for homeland defense and civil support. We are examining DOD's civil support capabilities in a separate report.

To determine the extent to which DOD has issued current and comprehensive guidance, we reviewed prior GAO reports and met with DOD officials to identify DOD's doctrine, policy, and strategy used for homeland defense and civil support. We reviewed homeland defense and civil support doctrine, policy, and strategy and other relevant documentation to assess the extent that it was current and identify any potential gaps, and met with officials from DOD and DHS to discuss the currency of the department's guidance and gaps in the guidance that may exist. To determine potential gaps in DOD's Strategy for Homeland Defense and Civil Support and the impact of any identified gaps, we compared the strategy against priorities articulated in current, overarching national- and department-level strategies and policies. To assess gaps within the dual-status commander construct and domestic cyber, we identified best practices in prior GAO reports and high-level DOD guidance, and to determine the extent that DOD demonstrated these practices, we interviewed DOD and DHS officials and reviewed related documents. More detailed information on our scope and methodology can be found in appendix I of this report.

We conducted this performance audit from November 2011 to September 2012 in accordance with generally accepted government auditing standards. Those 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.

Background

DOD's Homeland Defense and Civil Support Missions

DOD conducts a number of homeland defense and civil support missions. Examples of DOD's homeland defense missions include defending against threats to the homeland from, among other things, international terrorism, the proliferation of weapons of mass destruction, and cyber operations aimed at DOD computer networks. Examples of DOD's civil

support missions include responding to major disasters and emergencies (both natural and man-made); restoring public health and services and civil order, such as animal/plant disease eradication and counterdrug operations; and providing support for national special events, such as the political conventions and international summits. See figure 1.

Figure 1: Examples of DOD's Homeland Defense and Civil Support Missions



Source: GAO analysis of DOD agencies' information.

DOD's Role in Civil Support Missions

DOD is a supporting agency which provides assistance to the lead federal agency for a specific civil support mission. DOD provides support to DHS and other federal agencies for the defense portion of the federal response to a major disaster or emergency or special event when (1) state, local, and other federal resources are overwhelmed or unique defense capabilities are required; (2) assistance is requested by the lead federal agency; or (3) U.S. Northern Command is directed to do so by the President or the Secretary of Defense. The federal government's response to major disasters and emergencies in the United States is guided by DHS's *National Response Framework*, which involves a tiered series of responses, beginning with local authorities, state authorities, and

outside assistance from other states.⁵ In accordance with the *National Response Framework* and applicable laws including the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act),⁶ various federal agencies may play lead or supporting roles, based on their authorities and resources, and the nature of the threat or incident. For example, DHS manages the federal response to terrorist attacks and major disasters. In some instances, national defense assets may be needed to assist DHS or another agency in the national response to an incident. Defense resources are committed after DOD is directed to do so by the President or the Secretary of Defense. When deciding to commit defense resources to a request for assistance by a lead federal agency, DOD officials evaluate the request against 6 criteria: legality, lethality, risk, cost, military readiness, and appropriateness of the circumstances.⁷ If it is determined that defense assistance is appropriate, typically U.S. Northern Command and U.S. Pacific Command are responsible for leading DOD's response within their designated areas of responsibility. In most cases, support will be localized, limited, and specific. Figure 2 illustrates relevant portions of the areas of responsibility for U.S. Northern Command and U.S. Pacific Command

⁵ The *National Response Framework*—formerly called the *National Response Plan*—is a national-level guide on how local, state, and federal governments respond to major disasters and emergencies. The framework is based on a tiered, graduated response; that is, incidents are managed at the lowest jurisdictional levels and supported by additional higher-tiered response capabilities as needed. Department of Homeland Security, *National Response Framework* (Washington, D.C.: January 2008).

⁶The Robert T. Stafford Disaster Relief and Emergency Assistance Act, Pub. L. No. 100-707 (1988) (codified as amended at 42 U.S.C. § 5121, et seq.).

⁷Joint Chiefs of Staff, Joint Pub. 3-28, *Civil Support*, II-4, (Sept. 14, 2007).

Figure 2: Relevant Areas of Responsibility for U.S. Northern Command and U.S. Pacific Command



Source: DOD.

DOD Organizations that Have Key Roles and Responsibilities in Homeland Defense and Civil Support

A number of DOD organizations have key roles and responsibilities in the homeland defense and civil support missions. The Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs serves as the principal civilian advisor to the Secretary of Defense and the Office of the Under Secretary of Defense for Policy on homeland defense and civil support matters, among other things. The Assistant Secretary of Defense for Global Strategic Affairs is the principal advisor to the Under Secretary of Defense for Policy and the Secretary of Defense responsible for formulating and coordinating DOD strategy and policy on issues such as countering weapons of mass destruction, nuclear deterrence and missile defense, cyber security and space policy. The Joint Staff oversees joint doctrine development within DOD, including the joint publications for homeland defense and civil support. U.S. Northern

Command and U.S. Pacific Command are the two DOD geographic combatant commands primarily responsible for carrying out DOD's homeland defense and civil support missions. U.S. Strategic Command and U.S. Cyber Command, a sub-unified combatant command under U.S. Strategic Command, coordinate with U.S. Northern Command and DHS for domestic incidents with a cyber component. The military services typically provide the personnel and equipment to carry out homeland defense and civil support missions.

Table 1 describes the DOD organizations that have key roles and responsibilities in homeland defense and civil support and the organizations' roles for these missions.

Table 1: DOD Organizations that have Key Roles and Responsibilities in Homeland Defense and Civil Support

Organization	Roles and Responsibilities
Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs	Serves as the principal civilian advisor to the Secretary of Defense and the Under Secretary of Defense for Policy on homeland defense activities, civil support, and Western Hemisphere security matters.
Office of the Assistant Secretary of Defense for Global Strategic Affairs	Serves as the principal advisor to the Under Secretary of Defense for Policy and the Secretary of Defense, responsible for formulating and coordinating DOD strategy and policy on countering weapons of mass destruction, nuclear forces and missile defense, cyber security and space issues, and according to DOD officials, works closely with other assistant secretaries of defense to coordinate strategy and policy in these areas.
Joint Staff	Oversees and advises on the department's joint training, exercises, professional military education, doctrine, concept development and policy development, including counterterrorism and cyber policy.
National Guard Bureau	Facilitates and coordinates with other federal agencies regarding the use of National Guard resources for operations conducted under Title 32.
U.S. Northern Command and U.S. Pacific Command	Plan, organize, and as directed execute homeland defense operations within their areas of responsibility and provide support to civil authorities at the federal, state, and local levels as directed.
U.S Strategic Command/ U.S. Cyber Command	Synchronize planning for cyberspace operations in coordination with other combatant commands, the military services, and as directed by appropriate federal agencies.

Source: GAO analysis of DOD directives and policies.

The Dual-Status Commander Construct

According to DOD officials, dual-status commanders—military officers who coordinate state and federal responses to events for civil support missions—have been used for select planned and special events since 2004. The National Defense Authorization Act for Fiscal Year 2012⁸ provided that a dual-status commander should be the usual and customary command and control arrangement in situations when the armed forces and national guard are employed simultaneously in support of civil authorities, including missions involving major disasters and emergencies. The Act indicates that, when an officer is appointed as a dual-status commander, he or she serves on federal active duty, sometimes referred to as Title 10 status, as well as on duty in or with the National Guard of a state, sometimes referred to as Title 32 status.⁹ A dual-status commander can be appointed in one of two ways: 1) an active duty Army or Air Force officer may be detailed to the Army National Guard or Air National Guard respectively,¹⁰ or 2) an Army or Air National Guard Officer may be called to active duty.¹¹ The Secretary of Defense must authorize, and the Governor must consent to, designation of an officer to serve as a dual-status commander. When operating in Title 32 status, National Guard personnel, including dual-status commanders, are under the command and control of the state governor. DOD and National Guard personnel operating in Title 10 status, including dual-status commanders, are under the command and control of the President and the Secretary of Defense. Dual-status commanders—whether Army National Guard, Air National Guard, Army or Air Force—exercise command on behalf of and receive orders from both the Federal and the state chains of command. The dual-status commander is the intermediate link between these two separate chains of command.

DOD and the Council of Governors are working together to implement the dual-status commander construct. The Council of Governors consists of 10 U.S. state governors who are appointed by the President to a two-year term.¹² The council's purpose is to strengthen the partnership between the state and federal governments to protect the country, its people, and

⁸Pub. L. No. 112-81, § 515 (2011).

⁹Title 10 and Title 32 are titles of the United States Code that govern the operations of the Department of Defense and the National Guard respectively.

¹⁰See 32 U.S.C. § 315.

¹¹See 32 U.S.C. § 325.

¹²The Council of Governors was established by Executive Order 13528 in January 2010.

its property. The council when called upon, provides views, information, and advice on matters involving the National Guard of the various states, homeland defense, civil support, synchronization and integration of state and federal military activities in the United States, and other matters of mutual interest pertaining to National Guard, homeland defense, and civil support activities.

DOD Supports DHS in Domestic Cyber Preparedness and Response

DHS leads interagency efforts to identify and mitigate cyber vulnerabilities, and DOD provides support to DHS in carrying out its responsibilities. DHS developed the interim *National Cyber Incident Response Plan*¹³, which outlines domestic cyber incident response coordination and execution among federal, state and territorial, and local governments, and the private sector.

Some DOD Homeland Defense and Civil Support Mission Guidance Is Outdated or Incomplete, and No Routine Process Exists to Ensure Regular Updating

DOD has issued numerous policies and guidance related to its homeland defense and civil support missions; however some of it is outdated or incomplete, and no process exists to ensure updates are made to its primary homeland defense and civil support strategy. Specifically, DOD's primary strategy for how it will respond to an attack on the homeland or provide support to civil authorities in the event of a major disaster or emergency has not been updated since 2005 and no process exists to require such updating. Further, DOD's existing homeland defense and civil support guidance does not incorporate important details related to the dual-status commander construct and the department's response to a domestic cyber incident, such as its roles and responsibilities. While gaps still exist with DOD's strategy and guidance related to the dual-status command and domestic cyber, DOD has contributed to some national-level homeland defense and civil support guidance. Table 2 shows some of the key department and national level policies and guidance DOD uses to plan for its homeland defense and civil support missions, and when the guidance was last issued or updated.

¹³Department of Homeland Security, *National Cyber Incident Response Plan, Interim Version*, (Washington, D.C.: September 2010)

Table 2: Some Key Department and National Level Policies and Guidance that DOD Uses for its Homeland Defense and Civil Support Missions

Guidance (agency that issued guidance)	Date issued or last updated
Strategy for Homeland Defense and Civil Support (DOD)	June 2005
Joint Publication 3-27, Homeland Defense (DOD)	July 2007
Joint Publication 3-28, Civil Support (DOD)	September 2007
Department of Defense Homeland Defense and Civil Support Joint Operating Concept (DOD)	October 2007
National Response Framework (DHS)	January 2008
DOD Directive 5111.13, Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (DOD)	January 2009
Joint Action Plan for Developing Unity of Effort (DOD, DHS, Council of Governors)	2010
National Cyber Incident Response Plan, <i>interim</i> (DHS)	September 2010
Department of Defense Strategy for Operating in Cyberspace	July 2011
Memorandum of Agreement between DOD and DHS regarding Cybersecurity (DOD and DHS)	September 2010
DOD Directive 3025.18, Defense Support to Civil Authorities (DOD)	December 2010
DOD Directive 5111.18, Assistant Secretary of Defense for Global Strategic Affairs (DOD)	June 2011
Department of Defense Concept of Operations for Dual-Status Commander (DOD)	February 2012

Source: GAO analysis of DOD and national level guidance and policies.

DOD Has Not Updated Its Homeland Defense and Civil Support Strategy and Does Not Have a Process to Ensure Such Updates

DOD has established processes to issue and regularly update its directives and joint publications for homeland defense and civil support missions, but the department has not updated its primary strategy for these missions—the *Strategy for Homeland Defense and Civil Support*—since it was initially issued in 2005, and it does not have a process similar to that for its directives and joint publications to do so.¹⁴ While DOD plans to issue an updated strategy in the fall of 2012 in response to a 2010 GAO recommendation and internal department discussions, it has not yet developed a process to assess the need for future updates. DOD Instruction 5025.01 *DOD Directives Program*, issued in 2007

¹⁴Department of Defense, *Strategy for Homeland Defense and Civil Support* (Washington, D.C.: June 2005).

(incorporating changes made in 2010), requires DOD organizations to review their directives, instructions, manuals, and administrative instructions prior to the 5th anniversary of their publication date to ensure that they are necessary, current, and consistent with DOD policy, existing law, and statutory authority.¹⁵ As a part of this process, the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs updated its guidance for defense support to civil authorities in December 2010 with the issuance of DOD Directive 3025.18. This directive replaced or supplemented several directives, one of which had not been updated since 1993.

The Joint Staff has also established a process to update joint doctrine.¹⁶ Joint Staff officials stated that joint doctrine should not be more than 5 years old to maintain relevancy, and at the time of our review the Joint Staff had identified as a goal to have 100 percent of the joint publications updated within the last 5 years. According to DOD officials, this process includes requesting feedback across DOD regarding the currency of joint publications every 2 years. In August 2010, the Joint Staff determined that the joint publication on homeland defense, Joint Publication 3-27¹⁷ needed a complete revision based on feedback they received from the joint doctrine development community.¹⁸ The joint publication on civil support, Joint Publication 3-28,¹⁹ is also being revised. U.S. Northern Command is leading efforts to update the 2007 joint publications on homeland defense and civil support in coordination with the Joint Staff and other members of the joint doctrine community. According to Joint Staff officials, the revised joint publications are expected to reflect changes in national and department priorities and incorporate lessons learned from exercises and events such as Hurricane Katrina in 2005.

¹⁵DOD Instruction 5025.01, *DOD Directives Program*, § 4.c (Oct. 28, 2007, incorporating change 2, Jul. 1, 2010). This instruction superseded a previous DOD directive on updating publications from 2004.

¹⁶Chairman of the Joint Chiefs of Staff Instruction 5120.02C, *Joint Doctrine Development System* (Jan 2012).

¹⁷Joint Chiefs of Staff, Joint Pub. 3-27, *Homeland Defense* (July 12, 2007).

¹⁸The joint doctrine development community consists of the Chairman of the Joint Chiefs of Staff, the Joint Staff, the military services, the combatant commands, the National Guard Bureau, the combat support agencies, and other select DOD organizations.

¹⁹Joint Pub. 3-28, *Civil Support* (Sept. 14, 2007).

Joint Staff officials told us that the publications are scheduled to be issued in May 2013.

In contrast, DOD's primary strategy for homeland defense and civil support is 7 years old. According to DOD's joint doctrine development instruction,²⁰ national military strategies, such as DOD's *Strategy for Homeland Defense and Civil Support*, and joint doctrine should be closely linked because strategies define the desired outcome for joint doctrine. Moreover, GAO's *Standards for Internal Control in the Federal Government* and prior GAO audit work state that, to be effective, guidance—including strategies—should be current and complete.²¹ In the intervening years since the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs issued the *Strategy for Homeland Defense and Civil Support*, key national- and department-level guidance has been issued and significant civil support events have occurred that are not reflected in the department's primary strategy. For example, the homeland defense and civil support strategy does not address U.S. Cyber Command's role in domestic cyber incidents because the command was established in 2009, 4 years after the issuance of the strategy. Additionally, DOD's homeland defense and civil support strategy does not incorporate the restructured Chemical, Biological, Radiological, and Nuclear Enterprise.

The Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs has made previous attempts to update its 2005 homeland defense and civil support strategy. However these attempts have been unsuccessful, in part, because DOD does not have a process similar to its process for joint doctrine for periodically assessing the currency of its strategy and ensuring that updates are completed in a timely manner. In 2010, we reported that DOD began a revision of the strategy in October 2008, but it was postponed due to the forthcoming change in presidential administrations.²² At that time, the office estimated

²⁰Chairman of the Joint Chiefs of Staff Instruction 5120.02C, *Joint Doctrine Development System* (Jan. 13, 2012)

²¹GAO, *Standards for Internal Control in the Federal Government*, [GAO/AIMD-00-21.3.1](#) (Washington, D.C.: Nov. 1, 1999).

²²GAO, *Homeland Defense: DOD Needs to Take Actions to Enhance Interagency Coordination for Its Homeland Defense and Civil Support Missions*. [GAO-10-364](#) (Washington, D.C.: Mar. 30, 2010).

the updated strategy would be completed in March 2011; however, in September 2011 the office reported to Congress that the strategy remained valid and stated that it would provide updates on its approach to homeland defense and civil support through instructions and directives.²³ In June 2012, officials in the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs told us that the homeland defense and civil support strategy is being updated and is scheduled to be reissued by the fall of 2012. These officials also stated that the revised strategy will incorporate guidance from current national and department-level strategies and policies, such as the 2012 *Strategic Defense Guidance*, and the 2011 Presidential Policy Directive on national preparedness,²⁴ among others. An outdated homeland defense and civil support strategy cannot fully inform joint planning efforts in several critical homeland defense areas, including domestic cyber operations and chemical, biological, radiological, and nuclear preparedness. Reliance on an outdated strategy that does not reflect the department's current vision and understanding of homeland defense and civil support might hinder DOD's ability to effectively plan for and respond to major disasters and other emergencies.

Gaps Remain in Guidance Concerning DOD's Dual-Status Commander Construct

DOD has issued some guidance on the dual-status commander construct; however, gaps remain concerning the use and availability of dual-status commanders. Dual-status commanders—military officers who serve as an intermediate link between the separate chains of command for state and federal forces—have authority over both National Guard forces under state control and active duty forces under federal control during a civil support incident or special event.²⁵ DOD has been using dual-status commanders for select planned and special events since

²³Department of Defense, Letter from Paul Stockton, Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs to Carl Levin, Chairman of the Committee on Armed Services, September 2011.

²⁴Presidential Policy Directive/PPD-8: *National Preparedness* (Mar. 30, 2011).

²⁵The governors of the affected states and the Secretary of Defense must first mutually agree on the appointment of a dual-status commander, and the dual-status commander must still respect the separate chains of command for both sets of forces. For example, the commander may not issue orders to federal military forces while acting pursuant to state authority or vice versa. The dual-status commander construct does not give the President command of state military forces, or the Governor of a state command of federal military forces.

2004. For example, DOD officials stated that dual-status commanders were appointed for the 2004 G-8 Summit in Atlanta, Georgia, the 2005 border security exercise Operation Winter Freeze along the U.S.-Canadian border, and the 2010 National Scout Jamboree at Fort A.P. Hill, Virginia. In addition to these planned events, DOD used the dual-status commander for the 2012 Colorado wildfire response.

DOD has coordinated with stakeholders at the state and federal levels to issue guidance for the dual-status commander construct. For example, in 2010, DOD worked with DHS, the Federal Emergency Management Agency, and the Council of Governors to develop the *Joint Action Plan for Developing Unity of Effort*.²⁶ The plan provides a framework for state and federal agencies to coordinate their response to domestic incidents and describes the general arrangement of the dual-status commander construct. Among other things, the plan discusses how dual-status commanders can respond to planned and unplanned events, and it identifies the need for specialized training and certification. In addition, according to DOD officials, from August 2011 to February 2012, DOD signed memoranda of agreement with 51 of 54 states and territories²⁷. Furthermore, in February 2012, U.S. Northern Command issued a concept of operations which, among other things, establishes criteria for dual-status commander designation and training requirements. U.S. Northern Command has also worked with the National Guard Bureau to establish a curriculum that includes a sequenced schedule of classes for dual-status commander training and certification.

Nevertheless, gaps in guidance remain because DOD has not yet developed comprehensive policies and procedures regarding the use and availability of dual-status commanders. The National Defense Authorization Act for Fiscal Year 2012 states that the dual-status commander “should be the usual and customary command and control arrangement” when federal military forces and National Guard forces are employed simultaneously in support of civil authorities in the United States.²⁸ However, DOD has not identified specific criteria and conditions

²⁶ Department of Defense, Council of Governors, Department of Homeland Security, *Joint Action Plan for Developing Unity of Effort* (Washington D.C.: 2010).

²⁷ The territories include Washington, D.C.; Guam; the U.S. Virgin Islands; and Puerto Rico.

²⁸ Pub. L. No. 112-81, § 515 (2011).

for when the Secretary of Defense would agree with the governors of the affected states to appoint a dual-status commander. Some combatant command officials told us that the dual-status commander construct may not be appropriate for all scenarios and that other existing command and control arrangements can be used in responding to certain major disasters or emergencies. For example, U.S. Pacific Command officials stated that in 2011 when the tsunami warning resulting from the earthquake that struck Japan was issued in Hawaii, no dual-status commander was appointed; rather, U.S. Pacific Command coordinated its response in Hawaii directly with that state's authorities.

Additionally, gaps in guidance remain for the use of dual-status commanders for incidents affecting multiple states and territories, including complex catastrophes, because DOD has not yet developed policies and procedures for these scenarios.²⁹ The *Joint Action Plan* cites the significant likelihood that DOD will be called on to support responses to major disasters and emergencies affecting multiple states and territories. The *Joint Action Plan* states that past multistate emergencies such as Hurricane Katrina demonstrate that a coordinated and expeditious state-federal response is crucial to saving and sustaining lives, and it indicates that DOD and the several states will address the use of the dual-status commanders for such scenarios. However, DOD's concept of operations does not address how to use a dual-status commander in these scenarios. According to DOD, they are continuing to work with the Council of Governors to address the use of dual-status commanders in complex catastrophes affecting multiple states.

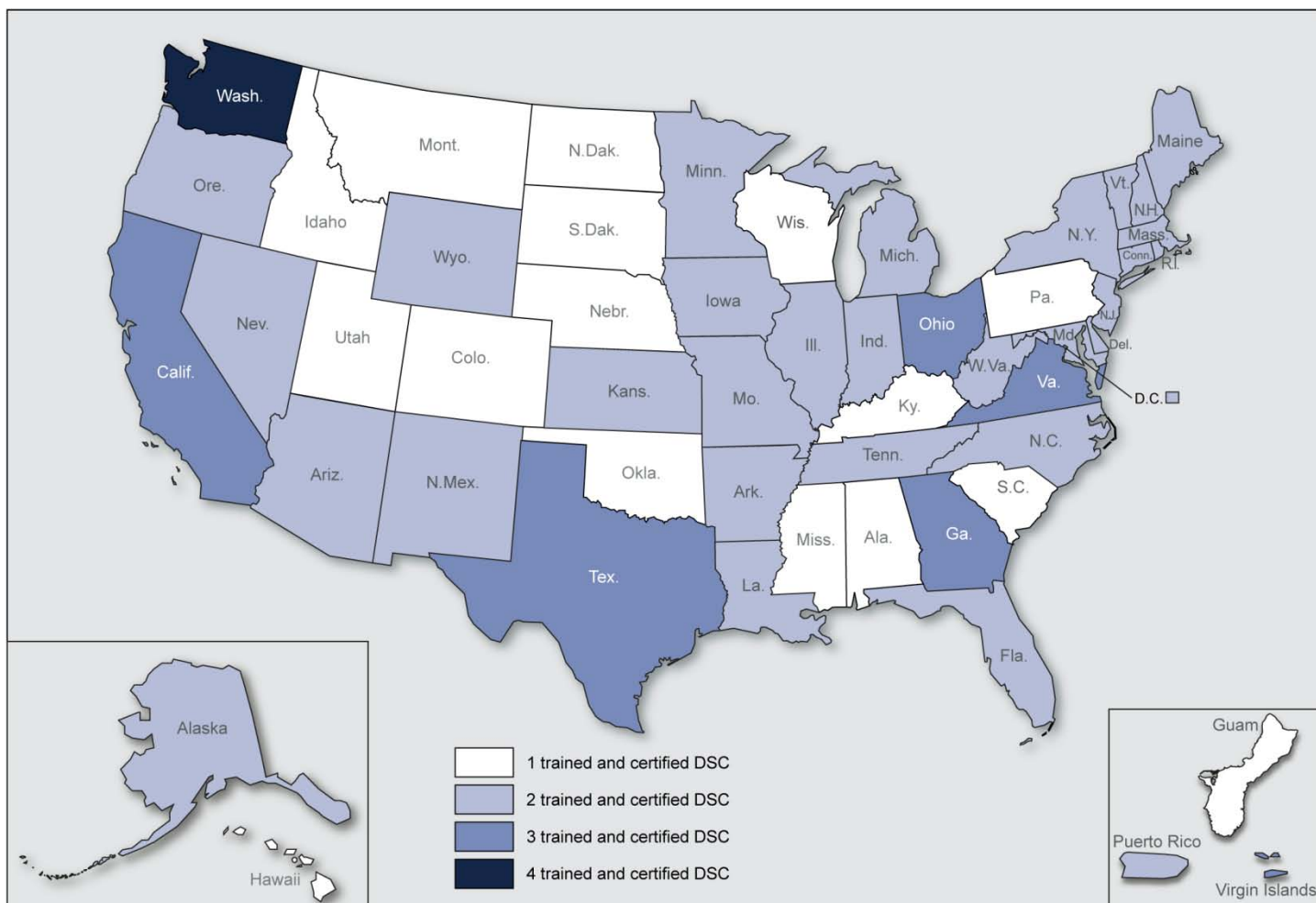
With respect to the availability of dual-status commanders, while DOD has a process for appointing dual-status commanders, it has not developed a process for determining the appropriate mix of National Guard and active duty federal officers. GAO's *Standards for Internal Control in the Federal Government*³⁰ emphasizes the importance of establishing policies and procedures to effectively manage resources to achieve desired results, such as the implementation of the dual-status commander construct. At the July 15, 2012 Council of Governor's

²⁹A complex catastrophe is an incident that has cascading effects, such as an earthquake that causes widespread casualties, displaces households, and damages major transportation and utilities such as electricity, water, and gas.

³⁰[GAO/AIMD-00-21.3.1](#).

meeting, the council and federal officials agreed to a goal of at least 3 trained and certified dual-status commander candidates with at least one being a general officer for each of the 54 U.S. states and territories, thus providing primary and alternate dual-status commanders. As figure 4 shows, all 54 U.S. states and territories have at least one trained and certified dual-status commander, 70 percent (38 of 54) have two or more trained and certified commanders, and 13 percent (7 of 54) have three or more commanders. As of June 2012, all of the trained and certified dual-status commanders shown in Figure 3 were National Guard officers.

Figure 3: Number of Trained and Certified Dual-Status Commanders in the 54 U.S. States and Territories, as of June 2012



Source: GAO analysis of DOD and National Guard data.

According to Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs and National Guard officials, maintaining a pipeline of trained and certified dual-status commanders drawn exclusively from the National Guard may be a challenge. The National Guard has a limited number of officers from which to select dual-status commanders, and these National Guard officers have other roles and responsibilities that may preclude them from being immediately available for an unplanned incident requiring a civil support response. For example, some individuals trained and certified to be dual-status commanders serve as airline pilots and may not be in the area when a

dual-status commander is needed. During Hurricane Irene in 2011, the trained and certified dual-status commander from one of the affected states was at a training exercise and unavailable. While the National Defense Authorization Act for Fiscal Year 2012 made it clear that dual-status commanders could be appointed from among the National Guard or active duty federal officers, as of May 2012, no active duty dual-status commanders have been trained and certified thus far. Office of Secretary of Defense and military service officials told us that it may be helpful to have an active duty federal dual-status commander for incidents affecting multiple states, such as a complex catastrophe. They stated that an active duty federal dual-status commander might have greater flexibility moving between multiple states and territories affected by an incident and might offer a broader, national perspective consistent with the Secretary of Defense's and the President's priorities. Training and certifying active duty dual-status commanders would increase the number of dual-status commanders and increase the likelihood that a dual-status commander will be available to serve when needed.

Without complete guidance on the use and availability of dual-status commanders, including when it is appropriate to deviate from the "usual and customary arrangement," it remains unclear when a different command and control arrangement would be more appropriate to provide a unity of effort between state and federal forces in civil support events. Also, without guidance on a process to determine the appropriate mix of individuals trained and certified to be dual-status commanders from the National Guard and active duty federal officers for the 54 U.S. states and territories, DOD's ability to adequately prepare for and effectively use dual-status commanders for a range of civil support events, including those affecting multiple states, may be hindered.

DOD Relies on its Broad Civil Support Guidance for Domestic Cyber Incidents

DOD has issued some guidance on preparing for and responding to domestic cyber incidents. DOD relies on its broad civil support mission guidance, which is also used for incidents such as responding to hurricanes and forest fires, to prepare for and respond to domestic cyber incidents. DOD Directive 3025.18, *Defense Support to Civil Authorities*, issued in 2010, describes how the department generally responds to requests for civil support and includes a broad description of the

department's roles and responsibilities for civil support.³¹ DOD's 2007 joint publication on civil support provides further details on the department's civil support mission, including an operational framework of how DOD prepares and responds to requests for assistance, a decision matrix for evaluating requests, and a broad description of the department's roles and responsibilities.³² In addition to the civil support directive and joint publication, in 2010 the Secretaries of Defense and Homeland Security signed a memorandum of agreement that outlines how the two agencies collaborate and coordinate cyberspace activities including those related to a domestic cyber incident.³³ Office of Secretary of Defense and DHS officials told us that the agreement has helped clarify the roles and responsibilities of the agencies.

Although DOD has some civil support guidance and an agreement with DHS for preparing for and responding to domestic cyber incidents, these documents do not provide some aspects of how DOD will support a domestic cyber incident. First, DOD's civil support mission guidance does not clearly define the department's roles and responsibilities during a domestic cyber incident. According to GAO's *Standards for Internal Control in the Federal Government*³⁴ and prior GAO audit work, effective guidance should be current, complete, and establish roles and responsibilities necessary to achieve an organization's missions and objectives. DOD's 2010 *Quadrennial Defense Review Report* acknowledges that DOD needs more clearly defined roles and responsibilities for operating in cyberspace. While DOD's guidance for its civil support mission broadly describes how the department can support other federal agencies during a civil support incident, DOD has not updated its civil support guidance to reflect current DOD cyber roles and responsibilities. For example, DOD's joint publication on civil support was issued 2 years before U.S. Cyber Command was established in 2009.

³¹Department of Defense Directive 3025.18, *Defense Support of Civil Authorities* (Dec. 29, 2010).

³²Joint Pub. 3-28.

³³Memorandum of Agreement Between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity (Oct. 12, 2010).

³⁴[GAO/AIMD-00-21.3.1](#).

In addition, the chartering directives for the Offices of the Assistant Secretary of Defense for Global Strategic Affairs and the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs³⁵ have assigned overlapping roles and responsibilities for preparing for and responding to domestic cyber incidents. Specifically, both DOD offices are responsible for coordinating and overseeing the department's cyber policy. Additionally, DOD's 2010 directive on civil support designates the Assistant Secretary of Homeland Defense and Americas' Security Affairs as the appropriate lead for civil support missions in general to include domestic cyber incidents. However, DOD officials told us that the Assistant Secretary of Defense for Global Strategic Affairs was the appropriate department lead for domestic cyber incidents and that this office was created after DOD published its 2009 chartering directive for the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs. DOD officials said they plan to omit the overlap when they update the 2009 directive. DOD officials told us that current national-level exercises involving DOD, DHS, and other federal agencies should help DOD clarify its roles and responsibilities and subsequently update its guidance for domestic cyber incidents. Nonetheless, until DOD clearly defines roles and responsibilities, the department risks a delayed response while its officials determine which entities to involve in responding to potentially time critical domestic cyber incidents. Moreover, multiple DOD entities may be performing overlapping planning functions, since it is not clear which office has lead responsibility.

Second, DOD has not taken adequate steps to ensure that its guidance aligns with national-level guidance and preparations for domestic cyber incidents. DOD has contributed to DHS national-level cyber response plans, including the *National Cyber Incident Response Plan* and the *National Response Framework's* Cyber Annex. However, DOD has not updated its own civil support mission guidance to ensure that it is consistent with national plans and preparations for domestic cyber incidents. Without guidance that aligns with national level plans and preparations, DOD's ability to support DHS during a domestic cyber incident could be hindered.

³⁵Department of Defense Directive 5111.18, *Assistant Secretary of Defense for Global Strategic Affairs* (June 13, 2011); and Department of Defense Directive 5111.13, *Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs* (Jan.16, 2009).

Conclusions

In the absence of clear and current guidance on DOD's critical and evolving homeland defense and civil support missions, DOD may continue to lack the ability to effectively plan and respond to incidents such as a domestic cyber attack or major disaster. While DOD has made some progress in issuing and updating relevant guidance to support its critical homeland defense and civil support missions, DOD still lacks the necessary framework for some of its most critical missions and a process to assess the currency of its strategy for these missions. Threats to the homeland and major disasters and emergencies, such as cyber attacks and earthquakes, frequently are unpredictable and occur with little or no notice. Maintaining up to date and comprehensive strategy and guidance will better position DOD to plan for and respond to myriad homeland defense threats and challenges. Without a strategy that accurately reflects the department's current approach to homeland defense and civil support, such as the creation of U.S. Cyber Command, DOD officials lack essential information to prepare for these critical missions. Further, while DOD's efforts to implement the dual-status commander construct could result in a more streamlined, comprehensive response to major disasters and emergencies, particularly those affecting multiple states and territories, until DOD clarifies how it plans to use dual-status commanders and develops a process for determining the appropriate mix of National Guard and active duty federal officers that it needs, the value of this construct will be diminished. Finally, without specific guidance on DOD's response to domestic cyber incidents, including clearly defined roles and responsibilities, DOD may be unable to quickly and effectively support DHS during domestic cyber attacks. As a result, DHS's ability to effectively respond to domestic cyber attacks and minimize their impact may be hindered. Enhancing DOD's overall preparedness, including developing and maintaining current and complete guidance for its homeland defense and civil support missions, would contribute to a more efficient national response to major disasters and emergencies and a more cost-effective use of federal resources for these critical missions.

Recommendations for Executive Action

The Secretary of Defense should direct the Under Secretary of Defense for Policy, acting through the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, to develop a process to periodically assess the currency of its *Strategy for Homeland Defense and Civil Support* and to ensure that updates, when needed, are completed in a timely manner.

The Secretary of Defense should direct the Under Secretary of Defense for Policy, acting through the Assistant Secretary of Defense for

Homeland Defense and Americas' Security Affairs and in collaboration with other appropriate stakeholders such as U.S. Northern Command, U.S. Pacific Command, and the National Guard Bureau, to develop implementation guidance on the dual-status commander construct that, at a minimum, includes:

- more specific criteria for determining when and how to use dual-status commanders, especially for civil support incidents affecting multiple states and territories and
- a process for determining the appropriate mix of National Guard and active duty federal officers to meet DOD's anticipated needs.

The Secretary of Defense should direct the Under Secretary of Defense for Policy to work with U.S. Strategic Command and its subordinate Cyber Command, DHS, and other relevant stakeholders to update guidance on preparing for and responding to domestic cyber incidents to align with national-level guidance. Such guidance should, at a minimum, include a description of DOD's roles and responsibilities.

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for review and comment. DOD concurred or partially concurred with all of our recommendations and stated that there are ongoing activities to address our recommendations. DOD's comments are reprinted in their entirety in appendix II. In addition, DOD provided technical comments, which we have incorporated into the report as appropriate.

DOD concurred with our recommendation that the Secretary of Defense direct the Under Secretary of Defense for Policy, through the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, to develop a process to periodically assess the currency of its *Strategy for Homeland Defense and Civil Support* and to ensure that updates, when needed, are completed in a timely manner. DOD stated that it recognizes the need to ensure that strategic guidance is clear and timely, and that going forward it will conduct an annual review to determine the currency of the homeland defense and civil support strategy. We believe that this review will better position DOD to plan for and respond to its critical homeland defense and civil support missions.

DOD also concurred with our recommendation that the Secretary of Defense direct the Under Secretary of Defense for Policy, through the Assistant Secretary of Defense for Homeland Defense and Americas'

Security Affairs and in collaboration with other appropriate stakeholders such as U.S. Northern Command, U.S. Pacific Command, and the National Guard Bureau, to develop implementation guidance on the dual-status commander construct. In its written response, DOD stated that the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs has drafted a DOD instruction that, among other things, establishes specific criteria for determining how and when to use dual-status commanders, as well as whom to authorize as dual-status commanders. We believe this instruction, when it is issued, will fill existing gaps in guidance on the use and availability of dual-status commanders that should result in a more streamlined, comprehensive department response to major disasters and emergencies.

DOD partially concurred with our recommendation that the Secretary of Defense direct the Under Secretary of Defense for Policy to work with U.S. Strategic Command and its subordinate Cyber Command, DHS, and other relevant stakeholders to update guidance on preparing for and responding to domestic cyber incidents to align with national-level guidance. In its written response, DOD agreed that some of its cyber guidance needs updating to ensure that the military services, combatant commands, and other DOD organizations are aware of their responsibilities relative to domestic cyber incidents. Although DOD acknowledged that there may be competing guidance within the chartering directives for the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs and the Assistant Secretary of Defense for Global Strategic Affairs, it stated that there is no confusion within the Office of the Secretary of Defense regarding who manages cyber policy. However, DOD did agree to further clarify cyber policy responsibilities when it next updates these two chartering directives. We believe that further clarification of DOD organizations' roles and responsibilities in guidance will enhance the department's ability to support DHS during significant domestic cyber incidents. We believe that DOD's response meets the intent of our recommendation.

We also provided a draft of this report to DHS for review and comment. DHS concurred with our recommendation that DOD coordinate with them to update guidance on preparing for and responding to a domestic cyber incident. DHS said it will coordinate with DOD as it updates its guidance. DHS's comments are printed in their entirety in appendix III.

As agreed with your offices, we plan no further distribution of this report until 1 day from the report date. At that time, we will distribute this report

to the Secretary of Defense and other relevant DOD officials. We are also sending copies of this report to interested congressional committees. The report is also available on our Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-4523 or at leporeb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in Appendix IV.

A handwritten signature in black ink, appearing to read "Brian Lepore". The signature is fluid and cursive, with the first name "Brian" and last name "Lepore" clearly distinguishable.

Brian J. Lepore
Director
Defense Capabilities and Management

Appendix I: Scope and Methodology

To determine the extent to which the Department of Defense (DOD) has issued current and comprehensive guidance, we reviewed homeland defense and civil support doctrine, policy, and strategy and other relevant documentation, and met with officials from DOD and Department of Homeland Security (DHS) to discuss the currency of the department's guidance and identify any potential gaps in the guidance that may exist. Specifically, we assessed national-level and DOD homeland defense and civil support guidance against emerging issues in our discussions with DOD, combatant command, and military service officials including the dual-status commander construct and domestic cyber. We also reviewed the assessments DOD received from the members of the joint doctrine community to determine which emerging issues prompted complete revisions of the joint publications on homeland defense and civil support and how these issues were addressed in other sources of guidance including directives, strategies, joint operating concepts, and national-level guidance. In addition, we reviewed recently issued GAO reports on homeland defense and civil support, and excluded potential gaps in guidance that were duplicative to those recently reported. Table 3 lists the offices we met with during this review.

Table 3: Offices We Met with During our Review

Name of Department	Office
Department of Defense	Office of the Under Secretary of Defense for Policy
	Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
	The Joint Chiefs of Staff
	Joint Directorate of Military Support
	Joint Directorate of Strategic Plans and Policy
	Joint Directorate of Joint Force Development, Joint Doctrine Branch
	U.S. Northern Command
	U.S. Army North
	U.S. Pacific Command
	U.S. Strategic Command
	U.S. Cyber Command
	U.S. Army
	Army War Plans Division
	U.S. Army Training and Doctrine Command
	U.S. Army Combined Arms Center
	U.S. Marine Corps
	Plans, Policies, and Operations
	U.S. Air Force
	Homeland Operations Division
	The National Guard Bureau
	The Army National Guard
Department of Homeland Security	Department of Homeland Security Policy
	Federal Emergency Management Agency's National Preparedness Directorate
	Federal Emergency Management Agency's Response Directorate
	National Cybersecurity and Communications Integration Center
	Office of Cyber Security and Communications
	National Cybersecurity Division
	United States Computer Emergency Readiness Team

Source: GAO

To determine potential gaps in DOD's *Strategy for Homeland Defense and Civil Support* and the impact of any identified gaps, we compared the strategy against priorities articulated in current, overarching national- and department-level strategies and policies—including the *National Response Framework*, the *National Security Strategy*, the January 2012

Defense Strategic Guidance, and the *Quadrennial Defense Review Report*. We also met with DOD officials and assessed relevant documentation, such as the instructions on joint doctrine development and updating directives, to determine the extent that the department had established and utilized a process to maintain current guidance. We used our assessment and discussion with DOD officials to determine the impact these established processes had on DOD's ability to maintain current doctrine and directives. Finally, we determined which key policy changes occurred since the strategy was released and the impact of not incorporating those changes in DOD's *Strategy for Homeland Defense and Civil Support*.

To assess gaps within the dual-status commander construct and domestic cyber, we identified best practices in prior GAO reports and high-level DOD guidance, and to determine the extent that DOD demonstrated these practices, we reviewed related documents, and we interviewed DOD and DHS officials. Specifically, we analyzed data provided by U.S. Northern Command, including the current number of individuals trained and certified as dual-status commanders and processes used to train and certify them. We used this data to determine how DOD was planning to use dual-status commanders and to what extent they determined the appropriate mix of active duty and National Guard dual-status commanders. We also assessed current guidance against information obtained in interviews with knowledgeable Joint Staff, Office of Secretary of Defense, combatant command, and military service officials to determine how DOD was planning to address identified gaps. To determine the currency and completeness of the department's guidance for domestic cyber incidents, we reviewed relevant guidance and met with DOD and DHS officials to discuss gaps and the impact of gaps on civil support for cyber incident responses. We determined which offices in DOD had a role for domestic cyber, reviewed relevant DOD directives outlining those roles, and analyzed whether there was any overlap within those offices or additional clarification that was needed. We compared this assessment to discussions with knowledgeable DOD and DHS officials to determine how DOD was planning to address any identified gaps.

We conducted this performance audit from November 2011 to September 2012 in accordance with generally accepted government auditing standards. Those 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: Comments from the Department of Defense



HOMELAND DEFENSE
& AMERICAS' SECURITY AFFAIRS

ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2600

SEP 14 2012

Mr. Brian Lepore
Director, Defense Capabilities and Management
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Lepore:

This is the Department of Defense response to the Government Accountability Office (GAO) report, "DOD Needs to Address Gaps in Homeland Defense and Civil Support," dated September 2012 (GAO Code 351666/GAO-12-965).

We acknowledge receipt of the draft report. We greatly appreciated the opportunity to provide an informal review of the report in August, and this collaborative approach greatly improved the quality and accuracy of this document. In addition to the response to the three recommendations from the draft report along with a version with sensitivity review mark-ups, my staff will supply administrative and substantive comments for your consideration via separate correspondence.

The Department looks forward to the opportunity to comment on the final report.

Sincerely,

Paul N. Stockton

Enclosures:

1. DoD Response
2. GAO Report with Sensitivity Review Mark-ups



**GAO DRAFT REPORT DATED AUGUST 2012
GAO-12-965 (GAO CODE 351666)**

**“HOMELAND DEFENSE: DOD Needs to Address Gaps in Homeland
Defense and Civil Support Guidance”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS**

RECOMMENDATION 1: The Secretary of Defense should direct the Under Secretary of Defense for Policy, through the Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs, to develop a process to periodically assess the currency of its *Strategy for Homeland Defense and Civil Support* and to ensure that updates, when needed, are completed in a timely manner.

DoD RESPONSE: Concur.

HD&ASA recognizes the need to ensure that strategic guidance is clear and timely, and for this reason its leaders regularly assess the strategic landscape to determine if an update to overarching guidance is required. For example, the 2012 Defense Strategic Guidance elaborated the Secretary’s new policy, operational, and fiscal priorities for the entire Department which, in turn, dictated that HD&ASA needed to adapt its overarching guidance on homeland-related issues to meet these strategic imperatives.

Going forward, HD&ASA will place the signed copy of the Strategy in OSD’s Staff Action Control and Coordination Portal (SACCP) with a one year due out to assess its currency. If deemed current, then it will be reentered into SACCP to allow for an annual assessment of the Strategy’s currency until a determination is made to update it. Conducting an annual review will be a tool to help HD&ASA ensure that its top-down strategic guidance remains up-to-date.

RECOMMENDATION 2: The Secretary of Defense should direct the Under Secretary of Defense for Policy, through the Assistant Secretary of Defense for Homeland Defense and Americas’ Security Affairs and in collaboration with other appropriate stakeholders such as U.S. Northern Command, U.S. Pacific Command, and the National Guard Bureau, to develop implementation guidance on the dual-status commander construct that, at a minimum, includes:

- More specific criteria for determining when and how to use dual-status commanders, especially for civil support incidents affecting multiple states and territories; and
- a process for determining the appropriate mix of National Guard and active duty Federal officers to meet DoD's anticipated needs.

DoD RESPONSE: Concur.

Based on a March 2012 Joint Staff Concept of Operations, the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs has drafted a DoD Instruction that provides policy and guidance on dual-status commanders. This Instruction establishes specific criteria for determining how and when to use dual-status commanders, as well as whom to authorize as dual-status commanders. This Instruction establishes requirements for U.S. Northern Command, U.S. Pacific Command, and the National Guard Bureau to maintain sufficient numbers of National Guard and Regular Army/Regular Air Force officers to serve as dual-status commanders. Formal coordination of this document is pending the ongoing work with the Council of Governors on the use of dual-status commanders in multi-state incidents, as well as incorporation of lessons learned from recent planned events and incidents in which dual-status commanders were authorized.

RECOMMENDATION 3: The Secretary of Defense should direct the Under Secretary of Defense for Policy to work with U.S. Strategic Command and its subordinate Cyber Command, DHS, and other relevant stakeholders to update guidance on preparing for and responding to domestic cyber incidents to align with national-level guidance. Such guidance should, at a minimum, include a description of DoD's roles and responsibilities.

DoD RESPONSE: Partially concur.

DoD concurs that certain guidance documents regarding preparing for and responding to domestic cyber incidents need updating as indicated by the GAO report. DoD will update documents as necessary to ensure components are aware of their responsibilities in supporting domestic cyber incidents. DoD has already established a very close working relationship with DHS and will continue to work these complex issues directly with DHS to ensure a whole-of-government approach to cyber security. Further, DoD will work directly with DHS and other Departments and Agencies in the final coordination and approval of the National Cyber Incident Response Plan (NCIRP). Final approval of the NCIRP will also inform DoD guidance documents and will serve as a catalyst for updating those documents at that time. Finally, DoD has worked very closely with the Administration, DHS, DoJ, and the other agencies of the government to better

understand the roles and responsibilities of key Departments and Agencies. That work is ongoing.

It is important to note, however, that although there may be competing guidance within the chartering directives for both the Assistant Secretary of Defense for Homeland Defense and America Security Affairs and the Assistant Secretary of Defense for Global Strategic Affairs, there is no confusion within the Department as to who manages cyber policy for the Department. The Office of the Deputy Assistant Secretary of Defense for Cyber Policy resides under the Office of the Assistant Secretary of Defense for Global Strategic Affairs who clearly manages cyber policy for the Department. It is also important to note that both Assistant Secretaries work for the Under Secretary of Defense for Policy and collaborate closely on all cyber security matters. From our perspective, the two chartering directives do not cause confusion now nor would they cause confusion in the future during a significant cyber incident. As DoD updates these chartering directives, appropriate language will be included to further clarify cyber policy responsibilities.

Appendix III: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

September 17, 2012

Brian J. Lepore
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: GAO Draft Report 12-965, "HOMELAND DEFENSE: DOD Needs to Address Gaps in Homeland Defense and Civil Support Guidance"

Dear Mr. Lepore:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the U.S. Government Accountability Office's (GAO's) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO highlighted DHS's role as the lead Federal agency for domestic cyber preparedness and response. The Department of Defense (DOD) provides support to DHS in carrying out its responsibility, which includes providing crisis management and coordination in response to a significant cyber incident. DHS has an interim National Cyber Incident Response Plan (NCIRP), which establishes the framework for organizational roles, and responsibilities, and actions to prepare for and respond to a domestic cyber incident, and is actively being used.

DOD and DHS also signed a Memorandum of Agreement (MOA) in September 2010 which established the Joint Coordination Element (JCE). The JCE has successfully enhanced the partnership and coordination efforts on cybersecurity operations and cyber incident responses between the Departments. In addition, the MOA has resulted in increased senior level dialogue across DOD and DHS, including the United States Cyber Command and the National Security Agency.

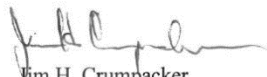
The draft report contained three recommendations which were directed specifically to DOD; however, Recommendation 3, with which DHS concurs, involved coordination between DOD and DHS. Specifically, GAO recommended:

Recommendation 3: The Secretary of Defense should direct the Under Secretary of Defense for Policy to work with U.S. Strategic Command and its subordinate Cyber Command, DHS, and other relevant stakeholders to update guidance on preparing for and responding to domestic cyber incidents to align with national-level guidance. Such guidance should, at a minimum, include a description of DOD's roles and responsibilities.

Response: Concur. DOD supports DHS's role in protecting the Federal domestic cyber preparedness and response efforts. Any coordination efforts associated with this recommendation should be directed to the DHS National Protection & Programs Directorate's Office of Cybersecurity and Communications (CS&C) or the JCE. DHS is pleased to engage and coordinate with DOD on updating their guidance on preparing for and responding to domestic cyber incidents.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,



Jim H. Crumpacker
Director
Departmental GAO-OIG Liaison Office

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Brian J. Lepore, Director, 202-512-4523 or leporeb@gao.gov

Staff Acknowledgments

In addition to the contact named above Marc Schwartz, Assistant Director; Katherine Arnold; Tommy Baril; Jennifer Cheung; Susan Ditto; Gina Flacco; William Jenkins; Jennifer Neer; Michael Silver; Amie Steele; and Michael Willems made key contributions to this report.

Related GAO Products

Homeland Defense: Continued Actions Needed to Improve Management of Air Sovereignty Alert Operations. [GAO-12-311](#). Washington, D.C.: January 31, 2012.

Homeland Defense and Weapons of Mass Destruction: Additional Steps Could Enhance the Effectiveness of the National Guard's Life Saving Response Forces. [GAO-12-114](#). Washington, D.C.: December 7, 2011.

Homeland Defense: Actions Needed to Improve Planning and Coordination for Maritime Operations. [GAO-11-661](#). Washington, D.C.: June 22, 2011.

Intelligence, Surveillance, and Reconnaissance: DOD Needs a Strategic, Risk-Based Approach to Enhance Its Maritime Domain Awareness. [GAO-11-621](#). Washington, D.C.: June 20, 2011.

Homeland Defense: DOD Needs to Take Actions to Enhance Interagency Coordination for Its Homeland Defense and Civil Support Missions. [GAO-10-364](#). Washington, D.C.: March 30, 2010.

Homeland Defense: DOD Can Enhance Efforts to Identify Capabilities to Support Civil Authorities during Disasters. [GAO-10-386](#). Washington, D.C.: March 30, 2010.

Homeland Defense: Planning, Resourcing, and Training Issues Challenge DOD's Response to Domestic Chemical, Biological, Radiological, Nuclear and High-Yield Explosive Incidents. [GAO 10-123](#). Washington, D.C.: October 7, 2009.

Homeland Defense: U.S. Northern Command Has a Strong Exercise Program, but Involvement of Interagency Partners and States Can Be Improved. [GAO-09-849](#). Washington, D.C.: September 9, 2009.

National Preparedness: FEMA Has Made Progress, but Needs to Complete and Integrate Planning, Exercise, and Assessment Efforts. [GAO-09-369](#). Washington, D.C.: April 30, 2009.

Emergency Management: Observations on DHS's Preparedness for Catastrophic Disasters. [GAO-08-868T](#). Washington, D.C.: June 11, 2008.

National Response Framework: FEMA Needs Policies and Procedures to Better Integrate Non-Federal Stakeholders in the Revision Process. [GAO-08-768](#). Washington, D.C.: June 11, 2008.

Homeland Defense: Steps Have Been Taken to Improve U.S. Northern Command's Coordination with States and the National Guards Bureau, but Gaps Remain. [GAO-08-252](#). Washington, D.C.: April 16, 2008.

Homeland Defense: U.S. Northern Command Has Made Progress but Needs to Address Force Allocation, Readiness Tracking Gaps, and Other Issues. [GAO-08-251](#). Washington, D.C.: April 16, 2008.

Continuity of Operations: Selected Agencies Tested Various Capabilities during 2006 Governmentwide Exercise. [GAO-08-105](#). Washington, D.C.: November 19, 2007.

Homeland Security: Preliminary Information on Federal Action to Address Challenges Faced by State and Local Information Fusion Centers. [GAO-07-1241T](#). Washington, D.C.: September 27, 2007.

Homeland Security: Observations on DHS and FEMA Efforts to Prepare for and Respond to Major and Catastrophic Disasters and Address Related Recommendations and Legislation. [GAO-07-1142T](#). Washington, D.C.: July 31, 2007.

Influenza Pandemic: DOD Combatant Commands' Preparedness Efforts Could Benefit from More Clearly Defined Roles, Resources, and Risk Mitigation. [GAO-07-696](#). Washington, D.C.: June 20, 2007.

Homeland Security: Preparing for and Responding to Disasters. [GAO-07-395T](#). Washington, D.C.: March 9, 2007.

Catastrophic Disasters: Enhanced Leadership, Capabilities, and Accountability Controls Will Improve the Effectiveness of the Nation's Preparedness, Response, and Recovery System. [GAO-06-903](#). Washington, D.C.: September 6, 2006.

Homeland Defense: National Guard Bureau Needs to Clarify Civil Support Teams' Mission and Address Management Challenges. [GAO-06-498](#). Washington, D.C.: May 31, 2006.

Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military's Response to Catastrophic Natural Disasters. [GAO-06-643](#). Washington, D.C.: May 15, 2006.

Hurricane Katrina: GAO's Preliminary Observations Regarding Preparedness, Response, and Recovery. [GAO-06-442T](#). Washington, D.C.: March 8, 2006.

Emergency Preparedness and Response: Some Issues and Challenges Associated with major Emergency Incidents. [GAO-06-467T](#). Washington, D.C.: February 23, 2006.

GAO'S Preliminary Observations Regarding Preparedness and Response to Hurricanes Katrina and Rita. [GAO-06-365R](#). Washington, D.C.: February 1, 2006.

Homeland Security: DHS' Efforts to Enhance First Responders' All-Hazards Capabilities Continue to Evolve. [GAO-05-652](#). Washington, D.C.: July 11, 2005.

Homeland Security: Process for Reporting Lessons Learned from Seaport Exercises Needs Further Attention. [GAO-05-170](#). Washington, D.C.: January 14, 2005.

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 website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://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 website, <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.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

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

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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

