

# Department of Homeland Security **Office of Inspector General**

**DHS Uses Social Media To Enhance Information  
Sharing and Mission Operations, But Additional  
Oversight and Guidance Are Needed**





**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

Washington, DC 20528 / [www.oig.dhs.gov](http://www.oig.dhs.gov)

September 5, 2013

MEMORANDUM FOR: Clark W. Stevens  
Assistant Secretary  
Office of Public Affairs

FROM:   
Assistant Inspector General  
Office of Information Technology Audits

SUBJECT: *DHS Uses Social Media To Enhance Information Sharing and Mission Operations, But Additional Oversight and Guidance Are Needed*

Attached for your information is our final report, *DHS Uses Social Media To Enhance Information Sharing and Mission Operations, But Additional Oversight and Guidance Are Needed*. We incorporated the formal comments from the Department in the final report.

The report contains five recommendations aimed at improving the effectiveness of the use of Web 2.0 technology. The Department concurred with recommendations 1 and 3, but did not concur with recommendations 2, 4, and 5. As prescribed by the *Department of Homeland Security Directive 077-01, Follow-Up and Resolutions for Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for each recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation.

Once the Department has fully implemented the recommendations, please submit a formal closeout request to us within 30 days so that we may close the recommendations. The request should be accompanied by evidence of completion of agreed-upon corrective actions.

Please email a signed PDF copy of all responses and closeout requests to [OIGITAuditsFollowup@oig.dhs.gov](mailto:OIGITAuditsFollowup@oig.dhs.gov). Until your response is received and evaluated, the recommendations will be considered open and unresolved. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Richard Harsche, Director, Information Management Division, at (202) 254-5448.

Attachment



## Table of Contents

Executive Summary.....	1
Background .....	2
Results of Audit.....	8
DHS Uses Social Media Effectively for Public Outreach .....	8
DHS Recognizes Value in Using Social Media To Enhance Mission Operations But Additional Oversight and Guidance Are Needed .....	12
Improvements Are Needed For Centralized Oversight and Coordination .....	16
Recommendations.....	19
Management Comments and OIG Analysis.....	19

## Appendixes

Appendix A: Objectives, Scope, and Methodology.....	25
Appendix B: Management Comments to the Draft Report .....	27
Appendix C: Major Contributors to This Report .....	34
Appendix D: Report Distribution.....	35

## Abbreviations

CBP	U.S. Customs and Border Protection
DHS	Department of Homeland Security
CISO	Chief Information Security Officer
FEMA	Federal Emergency Management Agency
ICE	Immigration and Customs Enforcement
GAO	Government Accountability Office
NIST	National Institute of Standards and Technology
NOC	National Operations Center
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPA	Office of Public Affairs



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

---

PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PTA	Privacy Threshold Analysis
TSA	Transportation Security Administration
USCG	U.S. Coast Guard
USCIS	U.S. Citizenship and Immigration Services
USSS	U.S. Secret Service



## **Executive Summary**

We audited the Department of Homeland Security's (DHS) efforts to implement Web 2.0 technology, also known as social media. The objective of our audit was to determine the effectiveness of DHS' and its components' use of Web 2.0 technologies to facilitate information sharing and enhance mission operations. The scope and methodology of this audit are discussed further in appendix A.

Although DHS prohibits social media access to employees using a government-issued electronic device or computer unless a waiver or exception is granted, the Department has steadily increased its use of various social media sites over the past 5 years. Specifically, the Department and each of its seven operational components have established accounts on commonly used social media sites, such as Twitter, Facebook, blog sites, and YouTube, for outreach purposes. Public affairs employees have had wide success using these sites to share information and conduct public outreach efforts. These initiatives were effectively managed and administered by Department and component level public affairs offices. In addition, component public affairs offices have implemented policies and procedures to provide guidance to employees.

DHS and its operational components have recognized the value of using social media to gain situational awareness and support mission operations, including law enforcement and intelligence-gathering efforts. However, additional oversight and guidance are needed to ensure that employees use technologies appropriately. In addition, improvements are needed for centralized oversight to ensure that leadership is aware of how social media are being used and for better coordination to share best practices. Until improvements are made, the Department is hindered in its ability to assess all the benefits and risks of using social media to support mission operations.

We are recommending that the Department communicate the process to gain access to social media; establish a list of approved social media accounts used throughout the Department; complete the Department-wide social media policy to provide legal, privacy, and information security guidelines for the approved uses of social media; ensure that components develop and implement social media policies; and establish a forum for the Department and its components to collaborate and make decisions on the use of social media tools.



## Background

The *Homeland Security Act of 2002* established the Department and its primary missions, which include preventing terrorist attacks within the United States; enforcing and administering the immigration laws of the United States; securing the nation's borders; and ensuring the nation's resilience to disasters. To support its mission operations, DHS relies on a vast array of information technology, including Internet-based services using Web 2.0 technologies.

Web 2.0 technologies, the second generation of the World Wide Web, provide a platform for Web-based communities of interest, collaboration, and interactive services. These technologies include Web logs, known as blogs, which allow individuals to post and respond to information. Additionally, Web 2.0 technologies include third-party social media websites that allow individuals or groups to create, organize, edit, comment on, and share information. DHS has defined social media as websites, applications, and Web-based tools that connect users to engage in dialogue, share information, collaborate, and interact.<sup>1</sup> Social media take many different forms, including Web-based communities, social networking sites, and video and photo sharing sites. Some commonly known social media providers include Facebook, Twitter, and YouTube.

Facebook is a social media website that allows users to create personal profiles and to locate and connect with other Facebook users. Users can also establish a page to represent a business, public figure, or organization. These pages are used to disseminate information and provide users a structure to post their responses. In September 2012, Facebook reportedly had more than 1 billion active users.

Twitter is a social networking site that allows users to share and receive information through short messages limited to 140 characters in length, known as "tweets." Twitter users can establish accounts, post messages to their profile page, and reply to other users' tweets. In December 2012, Twitter reported having 200 million registered accounts.

YouTube is a video-sharing site that allows users to watch, add, comment on, and share videos. Users can establish accounts on YouTube by providing a small amount of personal information. More than 800 million unique users visit the site, and more than 4 billion hours of video are watched each month.

---

<sup>1</sup> Department of Homeland Security Instruction 110-01-001, *Privacy Policy for Operational Use of Social Media*, June 8, 2012.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

The popularity of Web 2.0 technologies continues to grow. In 2011, nearly four in five active Internet users visited social media websites and blogs, and Americans spent more time on Facebook than any other website.<sup>2</sup> The Nielsen Company reported that, in July 2011, Americans spent more than 88 billion minutes on social media sites, and that number increased to more than 121 billion minutes in July 2012.<sup>3</sup> The use of social networking services now reportedly exceeds Web-based e-mail usage, and the number of American users frequenting online video sites has more than tripled since 2003. Overall, as of 2011, Americans spent 23 percent of their time online visiting blogs and social media websites.

#### Federal Guidance for Open Government

President Barack Obama endorsed the use of Web 2.0 technologies by Federal agencies in a 2009 memorandum promoting transparency and open government.<sup>4</sup> In this memorandum, Federal agencies were encouraged to use new technologies to put information about their operations online so that it would be more accessible to the public. Agencies were also encouraged to solicit public comments by providing opportunities for the public to contribute ideas and expertise through collaboration.

The President called on the Office of Management and Budget (OMB) to issue guidance for increasing government transparency and collaboration. In response, OMB has issued a number of guidance documents, including:

- *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*, issued April 7, 2010, which explains when and how the Paperwork Reduction Act of 1995 applies to social media.<sup>5</sup>
- *Guidance for Online Use of Web Measurement and Customization Technologies*, issued June 25, 2010, which explains how Federal agencies can use Web measurement and customization technologies to better serve the public while still safeguarding privacy.<sup>6</sup>
- *Guidance for Agency Use of Third-party Websites and Applications*, issued June 25, 2010, which states that the use of Web 2.0 technologies requires vigilance to

---

<sup>2</sup> A blog is a website that consists of a series of entries arranged in reverse chronological order, updated frequently with new information about particular topics. It often contains the writer's own personal experiences, opinions, and observations, or those of guest writers.

<sup>3</sup> The Nielsen Company provides information and measurement that enable companies to understand consumers and consumers' behaviors.

<sup>4</sup> President Barack Obama, *Memorandum on Transparency and Open Government*, January 21, 2009.

<sup>5</sup> OMB Memorandum, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act*, April 7, 2010.

<sup>6</sup> OMB M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, June 25, 2010.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

protect individual privacy and provides guidance to agencies to protect privacy when using social media websites.<sup>7</sup>

Federal agencies are increasingly using Web 2.0 technologies, such as social media websites, to share information, collaborate with the public, and increase transparency. As of May 2012, all 24 major Federal agencies had established a social media presence. For example, the National Aeronautics and Space Administration had as many as 3.3 million followers on Twitter. DHS activated a Twitter account in 2010 and, by November 2012, had 118,977 Twitter followers and had issued 2,796 tweets.

While the use of social media technologies can effectively engage the public and increase citizen involvement in government efforts, these technologies can also pose challenges in protecting personal information and ensuring the security of information systems.

Determining how the *Privacy Act of 1974*, as amended, applies to departmental use of social media requires careful evaluation.<sup>8</sup> This Act protects personally identifiable information (PII) by ensuring that Federal agencies collect only necessary and relevant information to an agency's function, and that the information is maintained in a manner that protects an individual's privacy. Examples of PII include name, date of birth, Social Security number, and any other unique information that could identify an individual. Because of the interactive nature of social media technologies, OMB requires that, in addition to following existing OMB guidance and privacy laws such as the Privacy Act, Federal agencies must have transparent privacy policies, provide notice for external website links, and conduct analysis of the privacy implications whenever they use third-party technologies to engage with the public.<sup>9</sup> For example, OMB states that an agency should post a privacy notice on a third-party website it uses to indicate whether and how the agency will maintain, use, or share PII. Agencies should also only collect the minimum necessary PII to perform their purpose or functions.

The rapid development of social media technologies presents challenges to keep up with evolving threats, such as unauthorized individuals gaining access to the enterprise network and identity theft. For example, the DHS Office of the Chief Information Officer (OCIO) reported that the use of these Internet-based technologies increases the risk of a malware infiltration, which may harm government systems or networks.<sup>10</sup> The Department conducted a risk assessment in 2012 and identified additional risks associated with employee use of social media technology, which cannot be monitored

---

<sup>7</sup> OMB M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010.

<sup>8</sup> 5 U.S.C. § 552a.

<sup>9</sup> OMB M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010.

<sup>10</sup> Malware is malicious software meant to interfere with or damage a computer or computer system.

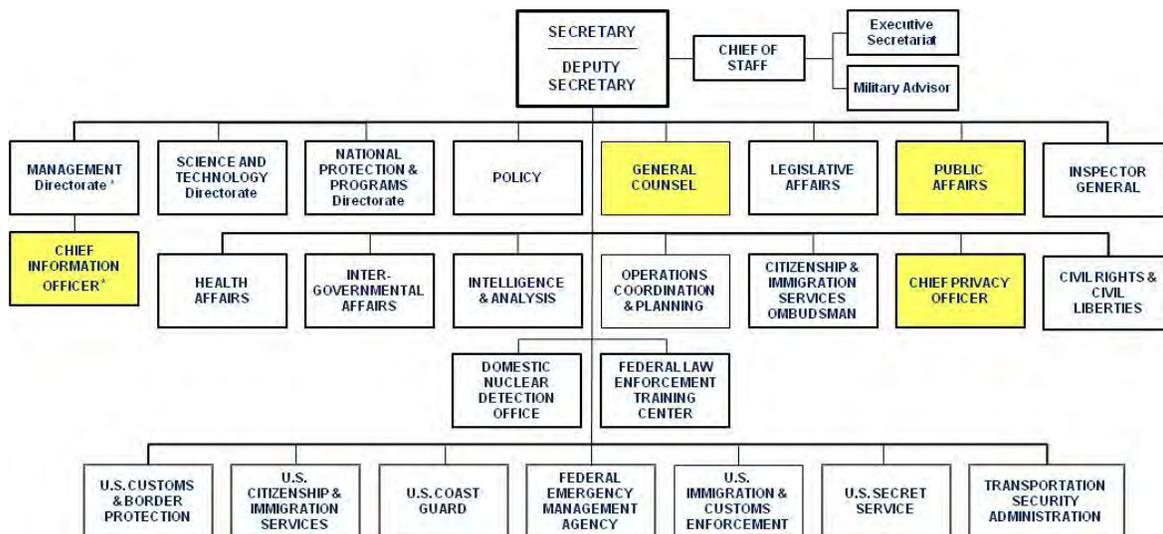


**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

by traditional methods.<sup>11</sup> The assessment also identified potential risks of security breaches, such as data spillage, reputation erosion, and loss of time and resources.

**Organizational Structure for Department-Wide Management of Social Media**

To address these risks, DHS has established an organizational structure to manage its Department-wide use of social media.<sup>12</sup> Four DHS offices share this responsibility. For the use of social media for outreach purposes, the DHS Office of Public Affairs (OPA) serves as the primary account holder for all DHS and component social media websites and ensures that posted content meets the appropriate requirements for publicly available information. The DHS Privacy Office is responsible for ensuring that DHS use of social media is compliant with privacy laws, while component level privacy offices are responsible for ensuring the implementation of DHS’ privacy policies. The DHS OCIO is responsible for providing overall policy implementation and procedural guidance for the Web and associated systems, and ensuring adherence to policies, laws, regulations, and guidance, including those that are related to accessibility, privacy, and security. The Office of General Counsel provides legal advice and guidance on the Department’s use of social media to all DHS components, including the DHS Privacy Office and component privacy offices. Figure 1 shows these four offices within the DHS organization.



**Figure 1. DHS Organization Chart as of 2012**

(\*The Management Directorate has six offices, including the Department’s Office of the Chief Information Officer)

<sup>11</sup> DHS Office of the Chief Information Security Officer, *Social Media Risk Assessment Report*, May 15, 2012.

<sup>12</sup> DHS Office of Inspector General (OIG) follows its own social media procedures and relies on its own attorneys, privacy officer, information security personnel, etc.



### **The Department Grants Access to Social Media Websites on a Limited Basis**

The Department is responsible for ensuring that employees who use social media are in compliance with Federal and departmental requirements for security of information systems. For example, the *Federal Information Security Management Act of 2002*, as amended, assigns agencies the responsibility for the security of information collected or maintained on their behalf and for information systems used or operated on their behalf.<sup>13</sup> Additionally, in 2009, the National Institute of Standards and Technology (NIST) issued guidance directing agencies to identify security controls for information systems for internal and third-party systems.<sup>14</sup> According to the guidance, the use of a risk-based approach is important when an agency is using technology for which its ability to establish security controls may be limited, such as when using a third-party social media service.

To limit its risk, DHS blocks social media sites from Department employees and contractors unless access approval is granted for official work purposes. DHS established a process in 2012 to grant access to employees whose job functions require the use of specific social media websites.<sup>15</sup> These employees must complete and submit a “Secure Internet Gateway” request to their component Security Operations Center. This request must include a business justification explaining the need to access specific blocked sites for work purposes. Component OCIO officials review the requests for technical accuracy and to validate that the business justification is in line with the component’s mission. Once the review is completed, the DHS Security Operations Center performs a risk assessment of the request to determine the level of risk to the DHS network and decides whether access should be granted.

Components may also request access to social media websites through a waiver or exception process. A waiver (valid for a specific timeframe) or exception (valid for an indefinite amount of time) is a request to bypass standard DHS security guidelines and policies, such as obtaining access to websites that are normally blocked. This process requires the approval of the component Chief Information Security Officer (CISO) and the DHS CISO. The Department had processed four exceptions and waivers as of 2012. Specifically, the Federal Emergency Management Agency (FEMA) was given waivers in 2010 and 2011 and applied for an additional waiver in 2012 to use social media to meet its mission requirements. U.S. Customs and Border Protection (CBP) was granted an exception for access to a specific website in 2009.

---

<sup>13</sup> FISMA, Title III, *E-Government Act of 2002*, Pub. L. 107-347, December 17, 2002, 44 U.S.C. § 3541, et seq.

<sup>14</sup> NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Revision 3, August 2009.

<sup>15</sup> Secure Internet Gateway Process V1.0, OIT DDC, December 4, 2012.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

Since 2007, the Department has been granting social media access on a case-by-case basis to support various public affairs or operational missions. Specifically, DHS uses social media to provide additional sources of communications to reach a wider audience, support operational activities such as investigations, and maintain situational awareness. The following describes these three categories of social media use.

- Communications comprises external communications, which include messaging, outreach, and public dialogue; and internal communications, which include the dissemination of key policy, procedural, and operational information to employees.
- Operational use includes the use of social media to collect information for the purpose of investigating an individual in a criminal, civil, or administrative context; making a benefit determination about a person; making a personnel determination about a Department employee; making a suitability determination about a prospective employee; or other official departmental purposes that has the potential to affect the rights, privileges, or benefits of an individual.
- Situational awareness includes information gathered from a variety of sources that, when communicated to emergency managers and decision makers, can form the basis for incident management decision making.



## **Results of Audit**

### **DHS Uses Social Media Effectively for Public Outreach**

---

Social media sites are a critical tool for DHS and its components to engage the public in DHS mission efforts, evidenced by a wide DHS presence on commonly used social media websites. The Department and components' public affairs offices have determined that the use of social media sites is more effective than static websites alone for external communications and public outreach. These efforts were effectively managed by Department and component level public affairs officials who had ample guidelines and procedures in place to ensure that employees follow protocol.

### **DHS Shares Information with the Public**

Social media sites have become an important method for DHS and its components to conduct outreach and share information with stakeholders. DHS began its first blog in 2007 to make information and services widely available, while promoting transparency and accountability. DHS components, such as U.S. Coast Guard (USCG) and FEMA, also began using social media websites as early as 2007 to communicate their mission accomplishments and provide informative tips to the public. Component public affairs officials told us that the use of social media has been steadily increasing since that time. As of November 2012, at least 395 employees had access to social media websites at DHS headquarters alone; and all seven operational components had established accounts on at least one of the most commonly used social media sites — Twitter, Facebook, blog sites, or YouTube — as shown in figure 2.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

CBP	FEMA	ICE	TSA	USCG	USCIS	USSS
 Twitter	 Twitter	 Twitter	 Twitter	 Twitter	 Twitter	 Twitter
	 Facebook	 Facebook		 Facebook	 Facebook	
	<b>Blog</b>	<b>Blog</b>	<b>Blog</b>	<b>Blog</b>	<b>Blog</b>	
 YouTube	 YouTube	 YouTube	 YouTube	 YouTube	 YouTube	

**Figure 2. Most Commonly Used Social Media Tools for Public Outreach<sup>16</sup>**

DHS and component public affairs offices have used social media tools to augment external communications and public outreach efforts. Representatives from the Department and component public affairs offices said that social media tools are more effective in generating awareness of DHS’ missions and achievements than static websites alone, helping DHS reach a wider audience. Officials also told us that the use of these tools provides a more formal process for measuring public interest through ongoing comments and interaction that was not possible before. Specifically, counting Facebook likes, YouTube views, comments posted and “retweets” can indicate how widely a particular posting is received.<sup>17</sup> For example, as of December 2012, USCG had more than 165,000 users following its Facebook page, and FEMA had more than 186,000 Twitter followers. The U.S. Citizenship and Immigration Services (USCIS) Office of Communications added a video of a mock citizenship interview and test to YouTube in November 2010, and the video had more than 522,000 views as of December 2012.

The Department has also reported on the importance of using social media to augment DHS’ emergency management communications. In testimony before the Senate Committee on Homeland Security and Governmental Affairs in May 2011, the FEMA Administrator said that social media is extremely valuable during disaster and emergency situations for its capabilities to collaborate with

<sup>16</sup> These icons represent the most common social media accounts used by CBP, FEMA, U.S. Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), USCG, USCIS, and U.S. Secret Service (USSS). DHS OIG does not endorse any non-governmental websites, enterprises, or services.

<sup>17</sup> The Facebook “like” button is a feature that allows users to show their support for specific comments, pictures, wall posts, statuses, or fan pages.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

individuals, communities, and emergency response stakeholders.<sup>18</sup> FEMA officials also reported that social media tools, such as Facebook and Twitter, are critical before disaster situations to provide preparedness information, as well as during and after disaster events to provide emergency management tips and specific instructions for victims. For example, following Hurricane Sandy in October 2012, FEMA's Office of External Affairs posted information on its Facebook site about new disaster recovery centers in the New York City area for residents to apply for assistance, charge cellular phones, and obtain food and water. The post also included an interactive link for a disaster recovery center locator. FEMA's Office of External Affairs has used Twitter since 2008, along with the FEMA blog since 2010, to communicate with the public and provide assistance to disaster survivors.<sup>19</sup>

Likewise, the USCG OPA has used Twitter and *The Coast Guard Compass*, the USCG blog, to provide the public with updates after disasters.<sup>20</sup> Fourteen Twitter accounts have been established across the USCG's district offices to provide information specific to local events. For example, a blog post in November 2012 outlined actions that that USCG had taken in response to Hurricane Sandy, such as efforts to restore fuel flow to the New York City area. The blog post also noted that prior to Hurricane Sandy, USCG worked to prepare Eastern seaboard ports to minimize disruption and emphasized USCG's commitment to restore the marine transportation system in the ports of New York and New Jersey. This blog post was shared 361 times.

Component public affairs employees frequently use Twitter, Facebook, and blogs to post time-sensitive information or specific news and current events. For example, the TSA Office of Strategic Communications and Public Affairs maintains a TSA Blog, which provides seasonal tips to help travelers deal with holiday-related issues, such as how to travel with food or how wrapped gifts may be subject to inspections.<sup>21</sup> Component officials also respond to questions frequently posted to blogs or Facebook sites. For example, the USCIS Office of Communications uses its blog, *The Beacon*, to address inaccurate information posted on immigration forums or prevent common mistakes made by

---

<sup>18</sup> U.S. Senate, Subcommittee on Disaster Recovery and Intergovernmental Affairs, *Understanding the Power of Social Media as a Communication Tool in the Aftermath of Disasters* (Statement of Craig Fugate, Administrator, FEMA), 112th Cong., 1st sess., May 5, 2011.

<sup>19</sup> <http://www.fema.gov/blog>

<sup>20</sup> *The Coast Guard Compass*, <http://coastguard.dodlive.mil/>

<sup>21</sup> *The TSA Blog*, <http://blog.tsa.gov/>



applicants.<sup>22</sup> A post on May 17, 2012, discussing the green card process, provided details about the decision process and timeline for applications.

### **DHS Established Guidelines To Administer Social Media Use For Public Outreach**

Department and component level public affairs officials effectively managed external communications and outreach efforts, respectively. DHS OPA, OCIO, and the Privacy Office provide Department-wide guidance for using social media for external communications. Specifically, the DHS OPA authorizes new social media accounts for the Department, in coordination with component public affairs offices, and negotiates terms of service for each social media site in coordination with the DHS Office of General Counsel. OPA also serves as the final authority over content acceptable for posting on social media sites when necessary and ensures that posted content meets the appropriate requirements for publicly available information and materials. The DHS CISO provides guidelines for rules of conduct as well as standards for social media accounts. For example, according to Attachment X of *DHS 4300A Sensitive Systems Handbook*, official accounts must be branded with the Department or component seal and use easily identifiable account user names that indicate that the user is representing DHS.<sup>23</sup> This handbook also includes tips to prevent employees from endorsing political parties or sharing classified information. Finally, the DHS Privacy Office requires component offices and programs to conduct a Privacy Threshold Analysis (PTA) for the use of third-party websites to assess whether PII is collected, stored, and managed. If the PTA results in a decision that a Privacy Impact Assessment (PIA) is required, the DHS Privacy Office works with the program to determine the privacy risks and mitigation of the use of the third-party website.

To comply with DHS privacy policies, OPA completed a PIA in 2010 to analyze the privacy risks associated with the Department's social media interactions. This PIA, *Use of Social Networking Interactions and Applications Communication/Outreach/Public Dialogue*, covered each of the Department's approved uses of social media for communications and public outreach.<sup>24</sup> A second PIA, *Use of Unidirectional Social Media Applications Communications and Outreach*, was completed in March 2011 for the use of unidirectional social media tools and applications that allow users to view real-time content from a

---

<sup>22</sup> *The Beacon*, <http://blog.uscis.gov/>

<sup>23</sup> Department of Homeland Security, *4300A Sensitive Systems Handbook Attachment X Social Media*, Version 9.1, July 24, 2012.

<sup>24</sup> This PIA currently covers 32 approved social networking applications.



predetermined source.<sup>25</sup> These two PIAs describe the Department's use of social media from a privacy standpoint.

Additionally, each of the seven operational components had established component level guidance and procedures for public affairs employees using social media for external communications. Specifically, six of the seven components had documented protocol for posting content, at least four components had documented privacy or comment policies, and at least four components had instituted specific guidance for employee use of social media for communications. For example, according to FEMA's December 2010 Web 2.0 policy, the FEMA Office of External Affairs has oversight of all external communications on FEMA's publicly accessible sites. The CBP OPA provided guidance, such as standard operating procedures to field employees, stating that officials in the field must first receive approval before posting content. CBP also issued a policy in 2012 explaining that social media posting is at the discretion of the CBP OPA.

---

**DHS Recognizes Value in Using Social Media To Enhance Mission Operations, But Additional Oversight and Guidance Are Needed**

---

The Department and its operational components have used social media tools to gain situational awareness and support mission operations, including law enforcement and intelligence-gathering efforts. Although social media sites have been beneficial for these activities, components did not have adequate guidelines or policies to prevent unauthorized or inappropriate uses of the technologies by employees. Recent efforts to establish privacy guidelines for operational uses of social media are progressing. However, additional component level policies and procedures are needed.

**Social Media Tools Prove Useful for Increasing Situational Awareness**

The Department recognizes that social media sites are a valuable resource for maintaining timely, accurate, and actionable situational awareness of potential and actual incidents that may require a response. DHS officials told us that the Department benefits from the speed and early warning that come with monitoring social media in conjunction with traditional media. For example, the DHS National Operations Center (NOC) is the primary watch center for situational awareness and is responsible for providing a common operating

---

<sup>25</sup> Unidirectional social media tools include mobile apps, podcasts, audio and video streams, short message service (SMS) texting, and really simple syndication (RSS) feeds, among others.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

picture and maintaining communications and coordination to prevent terrorist attacks and manage incidents. To do this, NOC personnel monitor media to discover and track incidents that may affect homeland security by using search terms to find items of potential interest across various websites and, starting in 2010, social media sites.<sup>26</sup> For example, in 2012, NOC staff monitored Twitter for updates on a police search for a man with a gun on the University of Maryland Baltimore County campus. NOC staff also monitored the Twitter accounts of multiple news organizations in 2012 to obtain information on a suspicious letter sent to the Speaker of the U.S. House of Representatives. With this type of real-time information, staff can provide notification and guidance on safety measures and other actions that should be taken.

Social media has also enabled FEMA Watch Centers to develop more timely situational awareness to communicate information to emergency managers and government officials and improve incident management decision making. FEMA's National Watch Center uses social media websites as an additional resource to maintain situational awareness of incidents that may require a coordinated Federal response. Watch Center personnel told us that they conduct searches to identify potential incidents that may predicate a coordinated Federal response. For example, the National Watch Center monitors social media during a storm to follow its progression and see how closely it matches the forecast and news reports. FEMA Watch Center staff also use this information to confirm the locations where weather events, such as tornado touchdowns, actually occurred.

### **Social Media Technologies Support Additional Mission Operations**

Some component program offices have increased the use of social media in law enforcement and intelligence-gathering activities to support DHS' mission. Using social media technologies, DHS personnel can interact with the public and gain access to additional information. Specifically, DHS law enforcement officials can use social media to gather information about suspects in criminal investigations. For example, ICE officials used social media to research a suspect during a child abuse investigation. Photos posted in the suspect's account revealed a license plate number and address, which enabled ICE to make a quick arrest. ICE officials told us that using social media for law enforcement purposes enables ICE employees to obtain information that is not always available through other means, such as law enforcement databases.

---

<sup>26</sup> The DHS National Operations Center is in compliance with DHS privacy policies for the use of social media for monitoring and situational awareness.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

DHS component program offices also use social media for intelligence-gathering activities to mitigate threats or formulate incident responses. For example, CBP border patrol agents review publicly accessible information from social media sites to gain awareness of potential situations at the border and to alert agents of safety concerns. Similarly, the TSA Office of Intelligence gathers information from several social media sites, including LinkedIn, YouTube, and others, to mitigate threats to the transportation sector, formulate incident responses, and meet situational awareness requirements.<sup>27</sup>

USSS officials told us that they are able to gain information through social media to help prevent potential incidents. Specifically, USSS uses social media to identify potential threats to protectees and protected events. For example, at the Republican National Convention in August 2012, the USSS learned through social media that a particular individual who had threatened to disrupt the event was in the area and relayed relevant information about that individual to the Protective Intelligence Coordination Center for further action.

#### Insufficient Guidance for Operational Use of Social Media

Although the Department has seen benefits from using social media to support mission operations, some components did not have specific guidelines or documented policies to ensure the proper use of these tools for situational awareness, law enforcement, or intelligence activities.

Personnel using social media to support mission operations told us that there was a need for additional policies or procedures that address the various challenges and questions relating to the use of social media. Component level procedures for employees who want to create new social media accounts for official purposes, or who are using social media for surveillance and interaction with individuals online, had not been developed. This has led to confusion as to what legal, privacy, and information security boundaries exist when using social media to perform operational tasks. For example, one program office used social media sites to monitor the activities of benefit applicants to help detect fraud. However, it was determined that the office did not have the proper authority to use social media for undercover work, and the use of social media was halted within the component.

Incidents of this nature led to the development of new departmental policies to ensure that DHS employees are aware of how social media technologies may be used for authorized activities. For example, in June 2012 the Department issued

---

<sup>27</sup> LinkedIn is a social networking website used for professional purposes.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

Directive 110-01, which established a formal privacy policy specifically for the operational use of social media to address access to and collection, use, maintenance, retention, disclosure, deletion, and destruction of PII.<sup>28</sup> The Directive also solidified roles and responsibilities for the Chief Privacy Officer, component heads, and component privacy officers, among others.

At the same time, the Privacy Office released Instruction 110-01-001, *Privacy Policy for Operational Use of Social Media*, to provide guidance for implementing Directive 110-01. The Instruction provides detailed definitions and Department-wide responsibilities associated with operational use of social media. The instruction also provides baseline “rules of behavior” for the operational use of social media, such as to use online screen names that indicate an official DHS affiliation while performing official tasks. To implement Directive 110-01, components were instructed to complete documents that specify the authority and purpose for each category of operational use of social media. Components were also instructed to establish their own rules of behavior to document operational use of social media, including date, site(s) accessed, information collected, and how that information was used. Components were instructed to develop training for the operational use of social media as well. Components were to provide this information to the Privacy Office for approval within 120 days from the release of the Directive. At the time of our audit, all seven component offices were in the process of developing and submitting the required documentation to the Privacy Office for approval. However, Privacy Office officials stated that stronger enforcement mechanisms are needed to ensure that components comply with this new Directive.

The DHS Office of Policy is drafting a Department-wide social media policy to define how social media may be used. At the time of our audit, the policy was undergoing internal review with departmental social media stakeholders. When implemented, this policy will provide formal roles and responsibilities for the Department’s social media stakeholders and leaders as well as a framework for official uses of social media to conduct communications, operations, intelligence activities, and situational awareness.

---

<sup>28</sup> DHS Directive 110-01, *Privacy Policy for Operational Use of Social Media*, June 8, 2012, excludes certain operational uses of social media for public outreach, situational awareness, and authorized intelligence activities.



## **Improvements Are Needed For Centralized Oversight and Coordination**

---

Although DHS components used social media to enhance information sharing and mission operations, the Department did not have a complete inventory of social media accounts, and some component employees had obtained access outside of the exception authorization process. In addition, DHS did not have a formal mechanism for sharing Department-wide best practices for using social media platforms. As a result, Department stakeholders had not yet achieved an understanding of how social media could be used more effectively to meet mission needs.

### **Department-Wide Social Media Usage Is Not Understood**

The Department could not fully account for how social media were being used. OMB requires Federal agencies to create a list of the third-party websites being used to communicate with the public.<sup>29</sup> To comply with this requirement, Department officials had attempted to establish a comprehensive inventory. OPA had begun to compile a list of official social media websites being used for communications and outreach in 2010. This list was organized according to social media platforms and listed at least 60 DHS accounts used to communicate with the public. However, at the time of our audit it was not clear how often this list was updated or who was responsible for updating the list. Similarly, the DHS Privacy Office developed a list of social media accounts for public outreach in 2010 as part of its privacy compliance process. The Privacy Office conducted its most recent compliance review in early 2012, which resulted in an inventory of 32 social media networking websites used for official DHS communications and outreach purposes.

However, the inventories prepared by OPA and the Privacy Office only listed social media websites being used for public outreach purposes. The Department could not produce a comprehensive, documented inventory for the operational uses of social media and what information is being collected by operational users. In August 2012 the DHS Privacy Office began an effort to identify and document components' operational uses of social media, as required by Instruction 110-01-001. As of November 2012, approximately 20 operational uses of social media had been identified across the seven operational components. However, these efforts were not completed at the time of our audit.

---

<sup>29</sup> OMB M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

Attempts to gain awareness of social media use have been hampered by employees who accessed websites outside of the standard process. Some DHS employees stated that they were not aware of the process to gain access or did not know where to go within the Department to request access to social media websites. Some employees told us they use nonstandard equipment, such as smart phones (e.g., iPhones), stand-alone personal computers, and home personal computers to conduct social media activities. For example, employees in one component office used their personal smart phones to gain access to social media websites to perform job duties.

Similar challenges exist for DHS to manage social media accounts effectively as they are established for new users or social media platforms. Although the DHS OPA is responsible for approving new social media accounts, this process was not always followed. Because most third-party social media sites require minimal information to create an account, component offices with the means to access these sites were able to proceed without obtaining authorization from DHS OPA. For example, Twitter only requires a person to enter his/her name, email address, and a password to create an account. DHS OPA officials told us that occasionally, unauthorized accounts are discovered once they are already active. OPA officials request that these accounts be removed. However, unauthorized accounts are rarely discovered.

#### **Better Coordination Is Needed To Share Social Media Practices**

Although using social media has proven beneficial, DHS did not have a formal mechanism to share best practices for using social media platforms. In 2010, DHS OPA established the New Media Compliance Steering Committee to increase coordination across headquarters and operating components; to ensure that social media tools and initiatives complied with Federal laws, regulations, and policies; and to apply standards consistently across the Department. The committee included representatives from all stakeholder offices, including the Office of General Counsel, Office for Civil Rights and Civil Liberties, Privacy Office, OPA, CISO, and Office of Records Management. OPA officials told us that this committee was effective in negotiating terms of service for new social media accounts and in identifying areas for improvement, such as websites that could be used to collect data to measure the success of the Department's social media use. However, the New Media Compliance Steering Committee was no longer operational at the time of our audit, and DHS had not established an alternative mechanism to coordinate social media efforts.

Without a committee or formal process to share information, DHS personnel cannot easily communicate or make decisions on how to use certain social media



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

platforms. Consequently, components using social media must conduct their own research when they want to try a new social media platform. DHS personnel in one program office said that they had to research which tool would be most effective to reach a community of practice for a system. These personnel believed that they could have saved time if a working group were in place to coordinate and exchange ideas. Sharing information between the components, rather than having each office and component conduct research separately, would increase efficiency.

In addition, without a centralized working group to share Department-wide best practices and lessons learned, personnel cannot be sure whether they are using the right social media tools or Web 2.0 technologies to their full capacity. Most component personnel told us that they reach out informally to other components with similar mission needs to learn about the different Web 2.0 technology options. However, most said that a formal working group would be helpful to increase communications and coordination.

Until the Department improves centralized oversight and coordination of social media use, stakeholders will not achieve a consolidated view of how the Department is using social media to conduct outreach and to support mission operations. Further, insufficient management oversight and coordination impedes efforts to institute Department-wide policies, standards, and procedures, leaving employees vulnerable to misuse of Internet technologies. Likewise, without a consolidated view of social media use, stakeholders cannot measure the effectiveness of various social media platforms to reach a wider audience or achieve specific DHS mission goals. Finally, the Department cannot fully assess the risks and challenges that components face when using certain social media sites, making it difficult to identify corrective actions or put improvement plans in place. Such actions would ensure that future social media technology use is allowed in a more structured and disciplined manner to support DHS' vast mission objectives.



## **Recommendations**

We recommend that the—

1. Office of Public Affairs, in coordination with the OCIO, communicate the Department's process for gaining access to social media for employees with an approved business need.
2. Office of Public Affairs, in coordination with the DHS Privacy Office, develop and maintain a list of approved social media accounts and owners throughout the Department.
3. Office of Policy complete the Department-wide social media policy to provide legal, privacy, and information security guidelines for approved uses of social media.
4. Privacy Office ensure that components develop and implement social media policies, as needed.
5. Office of Public Affairs establish a forum for the Department and its components to collaborate and make decisions on the use of social media tools for public affairs purposes, and that the DHS Privacy Office, in coordination with the Office of Operations Coordination and Planning, establish a forum for the Department and its components to collaborate and make decisions on the use of social media tools for operational purposes.

## **Management Comments and OIG Analysis**

We obtained written comments on a draft of this report from the Acting Chief Privacy Officer for DHS. We have included a copy of the comments in their entirety in appendix B.

In the comments, the Acting Chief Privacy Officer stated that the Department has significant concerns regarding the accuracy of the report and the recommendations as drafted. Specifically, the Acting Chief Privacy Officer stated that the report mischaracterized the Department's Directive 110-01; did not accurately represent the work done to implement the Directive; and portrayed a lack of Department-wide guidance regarding the use of social media. The Acting Chief Privacy Officer provided comments on specific areas within the report to



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

address these concerns. We have reviewed the Acting Chief Privacy Officer's comments, as well as technical comments submitted under separate cover, and made changes to the report as appropriate. However, we disagree with issues that the Acting Chief Privacy Officer raised in the response to our draft report. The following is an evaluation of the issues raised, as outlined in the Department's comments.

In the comments, the Acting Chief Privacy Officer had concerns with the "OIG's characterization that components did not have adequate guidelines or policies to prevent unauthorized or inappropriate uses of technologies by employees." The Acting Chief Privacy Officer stated that Directive 110-01 and its corresponding Instruction 110-01-001 establish a privacy policy for the operational use of social media for the Department. Although Directive 110-01 and Instruction 110-01-001 provide such Department-wide policy, the requirements of the Directive had not been fully implemented.

The Acting Chief Privacy Officer disagreed with the OIG's conclusion that additional component level policies and procedures are needed. The Acting Chief Privacy Officer stated that this conclusion minimizes the substantial compliance efforts of DHS components since Directive 110-01 was issued. Our conclusion is based on the fact that the full implementation of social media policies and procedures is not complete. We would note that in his comments, the Acting Chief Privacy Officer appears to support this conclusion when he writes that the DHS Privacy Office had approved social media documentation for "nearly all" components and that "nearly all" components have implemented the new training required by the Directive. The term "nearly all" suggests to us that more work is needed.

While Directive 110-01 and Instruction 110-01-001 provide a comprehensive privacy policy for operational use of social media, it also requires all DHS employees to obtain approval for each category of operational use of social media and to complete privacy training. As stated in our report, we determined that "some components did not have specific guidelines or documented policies." We also noted in the report that "at the time of our audit, all seven component offices were in the process of developing and submitting the required documentation to the Privacy Office."

Finally, the Acting Chief Privacy Officer emphasized that the DHS Privacy Office established standards, through Directive 110-01, for the use of social media that incorporate privacy protections and transparency. Specifically, the DHS Privacy Office published three Privacy Impact Assessments, as well as five Privacy Compliance Reviews. The audit report recognizes these accomplishments by



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

stating that “DHS has established guidelines to administer social media for public outreach” and cites the two Privacy Impact Assessments completed for public outreach purposes. The report also recognizes the Privacy Impact Assessment and Privacy Compliance Reviews completed for the DHS National Operations Center.

#### **Report Recommendations**

In the comments provided, the Acting Chief Privacy Officer concurred with Recommendations 1 and 3 and did not concur with Recommendations 2, 4, and 5.

In response to Recommendation 1, the Acting Chief Privacy Officer concurred and stated that the Department has established a process for employees with an approved business need to obtain access to social media. In response to the recommendation, the DHS Office of Public Affairs, in coordination with the DHS Chief Information Officer, will make the access process available on the DHS Intranet. Further, component level processes for gaining access to social media will be added to the DHS Intranet along with links to component Intranet sites. Finally, the Office of Public Affairs will revise the social media page on the DHS Intranet to reflect all recent updates and guidance for the appropriate use of social media across the Department.

We recognize the plans and efforts made to increase Department-wide communications of the process for gaining access to social media since our review. We look forward to receiving an update which outlines how the social media access process was communicated to all Department employees. OIG considers this recommendation Open-Unresolved.

In response to Recommendation 2, the Acting Chief Privacy Officer did not concur with our recommendation to develop and maintain a list of approved social media accounts and owners throughout the Department on the basis that a list for public affairs purposes already exists. Specifically, the Acting Chief Privacy Officer stated that the Office of Public Affairs collects information about each account during the application process for social media accounts. Although the Office of Public Affairs has begun to compile a list of social media accounts and websites used for outreach purposes, we determined that multiple inventories had been established by separate offices, with no clear plan for when or how the lists would be updated or maintained.

With regard to the operational use of social media, the Acting Chief Privacy Officer stated that maintaining such an inventory would compromise security



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

and investigative integrity. The Acting Chief Privacy Officer suggests that lists for operational use of social media be maintained by business owners within each component instead.

We do not agree with the Acting Chief Privacy Officer on this issue. As stated in our report, we recommend the Department develop and maintain a list of approved social media accounts and owners throughout the Department. Such a list may be established by business owners at the component level, then consolidated in a secure manner, as the Department determines appropriate. The Department operates a wide-area network that is secure at the sensitive but unclassified level, and it provides guidance and tools for components to protect their respective databases. Until the Department gains a consolidated view of social media use, it cannot measure the effectiveness of specific social media platforms to reach a wider audience and achieve various DHS mission goals, or ensure that security, privacy, and other risks are being fully addressed. OIG considers this recommendation Open-Unresolved.

In response to Recommendation 3, the Acting Chief Privacy Officer concurred with our recommendation to complete the Department-wide social media policy to provide legal, privacy, and information security guidelines for approved uses of social media, provided that the Department-wide social media Directive is consistent with DHS privacy policies and guidance and other existing Department policies. The Acting Chief Privacy Officer also mentioned that *DHS 4300A Sensitive Systems Handbook, Attachment X* provides guidance regarding the use of social media for public affairs purposes as well as required information security guidelines for uses of social media. OIG considers this recommendation Open-Unresolved.

In response to Recommendation 4, the Acting Chief Privacy Officer did not concur with our recommendation to ensure that components develop and implement social media policies, as needed. The Acting Chief Privacy Officer stated that Directive 110-01 and Instruction 110-01-001 provide for implementation for operational use of social media. Specifically, implementation of the Instruction requires each component to complete templates, along with specific rules of behavior and training of employees prior to engaging in operational use of social media. The Acting Chief Privacy Officer clarified in the comments that the DHS Privacy Office received 16 component templates and approved 13 of those templates before our fieldwork ended in November, 2012. According to the Acting Chief Privacy Officer, the remaining three templates were approved in December 2012.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

The Acting Chief Privacy Officer stated that by the conclusion of fieldwork in November, not all component templates had been reviewed or approved by the Privacy Office. During our fieldwork, we determined that some component employees using social media for operational purposes expressed a need for more Departmental or component level guidance. Other component employees with whom we spoke had concerns about the Directive, such as how social media was being defined, or that it would impede operational tasks performed with social media tools. Further, as the Acting Chief Privacy Officer stated in the comments, implementation of Directive 110-01 and Instruction 110-01-001 includes training employees prior to engaging in operational use of social media. However, many component employees with access to social media had not heard of the training or had not yet seen the training provided by the Privacy Office. None of the employees we spoke with had completed the training required by the Directive.

In our report, we recognize the efforts by several components in responding to the requirements of the Directive as well as in developing additional component level policies for employees using social media. We also recognize the efforts of the DHS Privacy Office for issuing the guidance and coordinating all compliance documentation. The Acting Chief Privacy Officer stated that this recommendation is unnecessary and creates redundant requirements for components. We do not agree with the Acting Chief Privacy Officer. This recommendation provides support to the Privacy Office in its efforts to compel components to develop and implement component-specific social media policies, as required by Directive 110-01. During our audit, DHS management reported a need for additional enforcement procedures to ensure that components comply with these policies. OIG considers this recommendation Open-Unresolved.

In response to Recommendation 5, the Acting Chief Privacy Officer did not concur with our recommendation to establish a forum for the Department and its components to collaborate and make decisions on the use of social media tools. Specifically, the Acting Chief Privacy Officer stated that the seven operational components have vast and diverse responsibilities, priorities, and missions, making it difficult to expect component social media will be the same. We understand there are different uses of social media across the Department. The three categories mentioned in the Acting Chief Privacy Officer's comments (communications and outreach, operational use, and situational awareness) were described in the Background section and throughout our report.

Although the Acting Chief Privacy Officer did not concur with this recommendation, in the comments, he provides evidence of DHS' commitment



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

to furthering collaboration for each use of social media. For example, the Acting Chief Privacy Officer states in his comments that the Office of Public Affairs will continue to work across the components to allow for the sharing of best practices on the use of social media in public affairs. The Acting Chief Privacy Officer also mentions multiple interactions between Headquarters and individual components, as well as existing component level working groups and information sharing methods already in place.

Further, contrary to the Acting Chief Privacy Officer's objection to this recommendation, we determined there is support for such a working group. Headquarters and component officials told us that a working group on social media would be helpful. Additionally, officials told us that a Department-wide working group had existed in the past, but disbanded when organizational changes took place in the Office of Public Affairs. Employees we spoke with said that the working group was beneficial as a method for sharing best practices on the use of social media. Such a forum would enable components and Headquarters staff to collaborate and enhance social media communication across DHS. OIG considers this recommendation Open-Unresolved.



## **Appendix A**

### **Objectives, Scope, and Methodology**

The DHS Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

As part of our ongoing responsibilities to assess the efficiency, effectiveness, and economy of departmental programs and operations, we conducted this audit to determine the effectiveness of DHS' and its components' use of Web 2.0 technologies to facilitate information sharing and enhance mission operations.

We researched and reviewed Federal laws and executive guidance related to the use of Web 2.0 technologies. We obtained published reports, documents, and news articles regarding the use of social media by the Federal Government, OMB, and DHS in particular. Additionally, we reviewed recent Government Accountability Office (GAO) reports to identify prior findings and recommendations regarding DHS' use of Web 2.0 technologies. We used this information to establish a data collection approach that consisted of focused interviews and documentation analysis to accomplish our audit objectives.

We held interviews primarily at DHS headquarters. We interviewed more than 15 DHS headquarters officials from the OCIO, OPA, the Office of Operations Coordination and Planning, the DHS Office of Policy, and the DHS Privacy Office to discuss their roles and responsibilities with regard to Web 2.0 technologies, the Department's use of social media, and the policies in place. We discussed security concerns and access controls and processes with the OCIO and OCISO. We met with OPA to learn more about using social media websites for communication and outreach. We discussed the use of social media for situational awareness purposes with the Office of Operations Coordination and Planning. We met with the DHS Office of Policy to learn about upcoming social media policies. To discuss privacy concerns and new privacy policies regarding the use of social media, we met with the DHS Privacy Office. We collected supporting documents about DHS' use of social media, Department-wide social media policies and procedures, information on DHS social media committees, and privacy documentation covering the current uses of social media by DHS operational components.

To assess the effectiveness of the Department's use of social media, we interviewed more than 25 officials from DHS' seven operational components—CBP, FEMA, ICE, TSA,



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

USCIS, USCG, and USSS—to learn how social media were being used, the policies currently in place, and the accessibility of third-party social media websites. We met with officials charged with overseeing and using social media at each of the seven components, including public affairs offices at six of the components, five component privacy offices, and officials at the OCISO at five components. Major component level Counsel Offices were also interviewed during the audit. Additionally, we met with component officials using social media for outreach, situational awareness, investigations, and intelligence purposes to learn more about the benefits and challenges of using Web 2.0 technologies.

We conducted audit field work from August to November 2012 at DHS Headquarters and operational component headquarters in Washington, D.C. We conducted this performance audit pursuant to the *Inspector General Act of 1978*, as amended, and according to the generally accepted government auditing standards. These 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions, based upon our audit objectives. The principal OIG points of contact for this audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, and Richard Harsche, Director of Information Management. Appendix C identifies major OIG contributors to the audit.



**OFFICE OF INSPECTOR GENERAL**  
Department of Homeland Security

**Appendix B**  
**Management Comments to the Draft Report**

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



**Homeland  
Security**

May 10, 2013

MEMORANDUM FOR: Frank Deffer  
Assistant Inspector General  
Office of Information Technology Audits

FROM: Jonathan R. Cantor   
Acting Chief Privacy Officer

SUBJECT: Response to *Office of Inspector General Draft Report: DHS Uses Social Media To Enhance Information Sharing and Mission Operations, But Additional Oversight and Guidance Are Needed – For Official Use Only (OIG Project No. 12-029-ITA-MGMT)*

Thank you for the opportunity to review and provide comments on the subject Draft Report, which includes observations and recommendations related to Department of Homeland Security's (DHS or Department) use of social media for a variety of purposes. We appreciate the Office of Inspector General's (OIG) work in planning and conducting its review and issuing this report. The Department has significant concerns regarding the accuracy of the subject report and Office of Inspector General's (OIG) recommendations as drafted.

Following a Privacy Office investigation into a Component's operational use of social media in a manner inconsistent with DHS privacy policy, the Privacy Office developed a draft Department-wide policy for operational use of social media. The Department subsequently issued this policy as Directive 110-01, *Privacy Policy for Operational Use of Social Media* (June 8, 2012). The Directive is in full effect across the Department. Per this Directive, the DHS Privacy Office is the lead on privacy policy for operational use of social media at the Department.

The Draft Report (1) mischaracterizes the breadth and applicability of Directive 110-01; (2) fails to accurately portray the work done to implement the Directive<sup>1</sup>; and (3) despite the existence of the Directive, maintains the inaccurate position that there is a lack of Department-wide guidance regarding the operational use of social media.<sup>2</sup>

<sup>1</sup> See specifically Recommendation 4: "Ensure that components develop and implement social media policies, as needed."

<sup>2</sup> See specifically Recommendation 3: "Complete the department-wide social media policy to provide legal, privacy, and information security guidelines for approved uses of social media."



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

The Privacy Office strongly disagrees with the OIG's characterization that "[c]omponents did not have adequate guidelines or policies to prevent unauthorized or inappropriate uses of technologies by employees" (Draft Report, page 12). Directive 110-01 and its corresponding Instruction 110-01-001 establish the privacy policy for operational use of social media by the Department. Employing the authorities of the Chief Privacy Officer, Component privacy officers, the Office of the General Counsel, and the Chief Information Officer, Directive 110-01 and its accompanying Instruction lay out a comprehensive framework for the protection of personally identifiable information (PII) when using social media and appropriate use of social media by Department personnel for operational purposes, including for situational awareness and law enforcement. The Instruction requires all DHS employees to comply with the Directive, privacy policies and procedures of the Chief Privacy Officer and applicable Component policies on the operational use of social media, and to protect PII from unauthorized use or disclosure.

The Privacy Office disagrees with the OIG's conclusion that while "[r]ecent efforts to establish privacy guidelines for operational uses of social media are progressing . . . additional component-level policies and procedures are needed" (Draft Report, page 12). This conclusion minimizes the substantial compliance efforts of DHS Components in the ten months since DHS issued Directive 110-01. The Privacy Office has received and approved Social Media Operational Use Templates ("Templates") and Rules of Behavior, as required by Directive 110-01, for nearly all Components whose personnel engage in the use of social media for operational purposes. With the exception of the U.S. Secret Service, which was granted an extension of the implementation deadline due to the Presidential election and Inauguration activities, nearly all operational Components have developed and implemented new training, as required by Directive 110-01. The U.S. Secret Service has subsequently completed training of their personnel. The DHS Privacy Office continues to work with Components to comply with the Directive and implement Component-wide policies.

The DHS Privacy Office established and enforces standards for the use of social media that incorporate privacy protections and are transparent. Directive 110-01 provides standards for Components to use social media for operational purposes while incorporating privacy protections. In addition, the DHS Privacy Office approved and published three Privacy Impact Assessments (PIA) on how the Department uses social media: two for the use of social media for communications and outreach purposes and one for the use of social media for situational awareness by the National Operations Center (NOC). The DHS Privacy Office has conducted five Privacy Compliance Reviews (PCR) as follow-ups to the NOC PIA; all five PCRs concluded that the NOC's use of social media was appropriate. Although the Department has been transparent regarding its use of social media, misperceptions still exist. Issuing a report that implies the Department's use of social media is not within regulatory or policy limits would pose significant potential harm to the Department's ability to conduct current and future operations.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

#### Department Response to Recommendations

The Department previously provided technical comments and corrections of factual errors to the OIG under separate cover. OIG recommends that the Deputy Under Secretary for Management work with the Office of Public Affairs, Office of Policy, Privacy Office, and Office of the CIO to:

**Recommendation 1:** Communicate the department's process for gaining access to social media for employees with an approved business need.

**Response: Concur.** The Department already has an established process for gaining access to social media through the Secure Internet Gateway (SIG). DHS employees with an approved business need can obtain a SIG request form by contacting DHS IT Support.

The Office of Public Affairs (OPA), in coordination with the Chief Information Officer (OCIO), will make available on the DHS Intranet all applicable details of the SIG process for gaining access to social media sites for employees with an approved business need. OPA recommends that Components provide input on how their employees can apply for access, which will be included on the DHS Intranet. Additionally, OPA encourages Component internal communicators to post links to the social media Intranet page on their respective Intranet sites, along with Component-specific information related to social media use. For example, the U.S. Secret Service developed a "Social Media" section on its Intranet, posting all relevant policies and directives governing the use of social media by USSS employees for operational and non-operational purposes.

To better communicate with employees regarding the appropriate use of social media and address this recommendation across the Department, OPA will revise the current social media page on the DHS Intranet to reflect any and all recent updates and include additional information and guidance, as well as relevant policy documentation. This page currently describes the use of social media across the Department, and details the application process for Components, programs, and offices that want to establish an official social media presence for public affairs purposes. The current Intranet page also houses the list of social media accounts utilized for public affairs purposes. Estimated Completion Date (ECD): October 1, 2013

**Recommendation 2:** Develop and maintain a list of approved social media accounts and owners throughout the Department.

**Response: Non-Concur.** A list of approved social media accounts for public affairs purposes already exists. Information about those who maintain an account for public affairs purposes exists for internal use only. OPA collects this information, including information about the account holder, the account password, and the intended use of the account, during the application process as part of its responsibility to oversee social media activity by Department public affairs personnel.

For other purposes, maintaining such information in a Department-wide list compromises security and investigative integrity, leading to the potential for a breach of the information.



## OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

---

Instead, lists will be maintained by business owners. For example, CBP's draft Directive for operational use of social media requires the business owner of the system through which social media access occurs to maintain an accounting of approved users and purposes.

Further, the Draft Report references Office of Management and Budget *Guidance for Agency Use of Third-Party Websites and Applications* (OMB M-10-23), June 25, 2010; however, the guidance does not require Departments to maintain an inventory of operational users of social media. Information about these accounts, which could include accounts for law enforcement purposes, and their intended uses, must be distributed only to those with a need to know and not be compiled in a single, Department-wide list.

**Recommendation 3:** Complete the Department-wide social media policy to provide legal, privacy, and information security guidelines for approved uses of social media.

**Response: Concur.** The Department concurs with this recommendation, provided that the Department-wide social media Directive is consistent with DHS privacy policies and guidance, Directive 110-01, and other existing Department policies. The Department will develop social media guidance to address the Department's many growing uses of social media to build on and enhance existing policies. It is important to note that Attachment X of DHS 4300A provides clear and succinct guidance to leverage regarding the use of social media for public affairs purposes, and required information security guidelines for approved uses of social media. ECD: December 2013

**Recommendation 4:** Ensure that components develop and implement social media policies, as needed.

**Response: Non-Concur.** Directive 110-01 and its accompanying Instruction provide for implementation for categories of operational use of social media. Implementation of the Instruction includes the completion of Templates, along with Component-specific Rules of Behavior, and Component-based training of employees prior to engaging in the operational use of social media. Templates document the current or proposed category of operational use of social media; identify the appropriate authorities for the category of use; describe what PII, if any, is collected (and from whom); and describe how the information is used. After initial Templates are approved, if Components determine to engage in, or contract for, new or modified categories of operational use of social media, the Instruction requires them to complete a new Template that includes Rules of Behavior and provides for any necessary training before the new category of use can be approved. The DHS Privacy Office reviews approved Templates every three years for accuracy.

Templates and draft Rules of Behavior for existing categories of operational use of social media were due to the DHS Privacy Office by October 12, 2012. Prior to the submission deadline, the DHS Privacy Office received sixteen completed Templates for review from Components. Of the sixteen completed Templates, thirteen were approved by the DHS Privacy Office by November 7, 2012, and provided to the Office of Inspector General as part of its fieldwork for this Draft Report, to demonstrate Component compliance with Directive 110-01. The remaining three Templates were approved by the DHS Privacy Office in December 2012.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

Directive 110-01 and its accompanying Instruction require Component Privacy Officers and Privacy Points of Contact to tailor privacy training for the operational use of social media based on Component-specific needs. The DHS Privacy Office provided a baseline training slide deck to the Components on July 23, 2012, for further tailoring by Components based on the category of operational use of social media. The Instruction requires Components to complete employee training by November 26, 2012. The DHS Chief Privacy Officer granted an extension of this deadline to the U.S. Secret Service due to the Presidential election and Inauguration and required U.S. Secret Service to complete its training by March 1, 2013. On February 6, 2013, the U.S. Secret Service Privacy Office sent an official message to Assistant Directors of several U.S. Secret Service directorates requiring employees whose positions may require the use of social media for operational purposes to complete mandatory privacy training on the operational use of social media.

Components have been developing social media policies and communicating requirements to their employees to adhere to Directive 110-01 since the Directive became effective and even before. For example, prior to the issuance of Directive 110-01, the U.S. Secret Service developed several internal directives governing the management of content on social media sites, standards of conduct for employees using social media, standards for use of social media for unofficial purposes, and provided guidance on privacy and mitigation issues concerning the use of social media on government equipment. In October 2012, the U.S. Secret Service Privacy Office sent an official message to all employees and supervisors notifying them of the newly-developed U.S. Secret Service privacy policy, which established Rules of Behavior governing the use of social media for law enforcement and non-law enforcement purposes.

The U.S. Coast Guard and U.S. Immigration and Customs Enforcement (ICE) circulated memoranda to their respective personnel detailing Rules of Behavior and responsibilities for using social media for operational purposes prior to granting access to the social media after Directive 110-01 was issued. In response to Directive 110-01, the U.S. Customs and Border Protection (CBP) Privacy Office drafted an internal Directive for Operational Use of Social Media memorializing the process for establishing Rules of Behavior, the method for gaining access to social media and the responsible parties, and the different levels of operational use of social media within CBP.

The DHS Privacy Office continues to receive Templates from Components as additional operational uses of social media are identified. To date, the DHS Privacy Office has approved three additional Templates for categories of operational use of social media.

Given that the Chief Privacy Officer approves Component-specific Templates and Rules of Behavior, and given appropriate training for the operational use of social media and the ongoing work done by Component Privacy Officers and Privacy Points of Contact to comply with Directive 110-01, this recommendation is unnecessary and creates redundant requirements for Components.



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

**Recommendation 5:** Establish a forum for the Department and its components to collaborate and make decisions on the use of social media tools.

**Response: Non-Concur.** DHS' seven operational Components, while serving the DHS mission at large, have vast and diverse responsibilities, priorities, and missions. For this reason, it is difficult to put seven operational Components under the same umbrella for the use of "Web 2.0" technology and to expect that Component uses will be the same across the board. The audit attempted to summarize all of the work of Headquarters and operational Components, which includes several law enforcement Components, a disaster recovery Component, and the Component that administers citizenship, into generic "DHS" work." As social media are used at DHS for three very distinct purposes—public affairs, situational awareness, and operational use—a generic forum for all social media practitioners fails to recognize the very different missions, needs, and operations of DHS' diverse Components and missions.

Regarding the situational awareness and operational uses of social media at the Department, this report acknowledges that there is not currently a formalized structure for discussions on the use of social media. Useful, educational, and informal communication does take place among operational users of social media at the Department, however, the Department remains committed to furthering such collaboration.

Creating a formal entity for social media public affairs practitioners to collaborate may promote consistent messaging and current best practices. Due to the Department's diverse and wide-ranging mission, however, as well as the ever-changing nature of social media, such an entity needs to be dynamic and not limited to in-person communication.

As the DHS mission is so diverse, it is logical for public affairs professionals to work together to ensure a "One DHS" message. In fact, public affairs employees from around Headquarters and across the operational and support Components constantly work together on both internal and external products, including social media.

Additionally, OPA will continue to work across Components to allow for the sharing of best practices on the use of social media in public affairs. Forums for collaboration on social media already exist, both internally and government-wide, and the Department will continue to seek new opportunities to network and collaborate on best practices.

As an example, DHS Headquarters public affairs works with counterparts at the following Components, among others:

- ICE, to inform the public about successful Homeland Security Investigations on social media channels.
- Federal Emergency Management Agency (FEMA) Headquarters, as well as staff in its 10 regions nationwide, to provide preparedness messaging to the public.
- U.S. Secret Service, to communicate information about upcoming National Security Special Events.

Many DHS Components are already utilizing forums, both formal and informal, to collaborate. For example, FEMA Headquarters utilizes the SharePoint tool to collaborate with its digital



## OFFICE OF INSPECTOR GENERAL

### Department of Homeland Security

---

communications staff located throughout the country in the FEMA Regional Offices, increasing efficiency, information sharing, and coordination. U.S. Citizenship and Immigration Services established a Social Media Working Group in May 2012 to develop component-wide policies related to operational use of social media and compliance with Directive 110-01, as well as to address evolving policy and issues related to social media use. The CBP Privacy Office's monthly compliance meetings with privacy liaisons and the CBP draft Directive on operational use of social media provide a framework for addressing component requirements and uses related to social media.

Furthermore, formalized tools for social media public affairs professionals currently exist, and are available to DHS employees at no cost. The General Services Administration (GSA) Center for Excellence in Digital Government "provides government-wide support and solutions that help agencies deliver excellent customer service to the public via web, social media, mobile, phone, email, print, and newly evolving media. These solutions include training via DigitalGov University; standards and best practices via [HowTo.gov](http://HowTo.gov); support to inter-agency communities of practice such as the [Federal Web Managers Council](http://FederalWebManagersCouncil.org); access to cost-cutting tools and technology; and research and analytics on citizen needs and expectations for better service. In addition, the Center is an accelerator and incubator for government-wide new media and citizen engagement solutions, making it easier for the government and the public to constructively engage via tools such as [Challenge.gov](http://Challenge.gov)." Additionally, the GSA-sponsored Social Media Community of Practice (SM-COP) is a collaborative forum for practitioners from across the government to share thoughts and ideas.

Thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you in the future.



## **Appendix C**

### **Major Contributors to This Report**

Richard Harsche, Division Director  
Kristen Bernard, Audit Manager  
Craig Adelman, Auditor-in-Charge  
Thea Calder, Auditor  
Beverly Dale, Referencer  
David Bunning, Referencer



## **Appendix D**

### **Report Distribution**

#### **Department of Homeland Security**

Secretary  
Deputy Secretary  
Chief of Staff  
Deputy Chief of Staff  
General Counsel  
Executive Secretary  
Director, GAO/OIG Liaison Office  
Assistant Secretary for Office of Policy  
Assistant Secretary for Office of Public Affairs  
Assistant Secretary for Office of Legislative Affairs  
DHS Chief Information Officer  
DHS Chief Information Security Officer  
Director, Office of Operations Coordination and Planning  
Acting Chief Privacy Officer  
CBP, Commissioner  
FEMA, Administrator  
ICE, Director  
TSA, Administrator  
USCG, Admiral  
USCIS, Director  
USSS, Director  
DHS OCIO Liaison  
CBP Liaison  
FEMA Liaison  
ICE Liaison  
TSA Liaison  
USCG Liaison  
USCIS Liaison  
USSS Liaison

#### **Office of Management and Budget**

Chief, Homeland Security Branch  
DHS OIG Budget Examiner

#### **Congress**

Congressional Oversight and Appropriations Committees, as appropriate

## ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this document, please call us at (202) 254-4100, fax your request to (202) 254-4305, or e-mail your request to our Office of Inspector General (OIG) Office of Public Affairs at: [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov).

For additional information, visit our website at: [www.oig.dhs.gov](http://www.oig.dhs.gov), or follow us on Twitter at: [@dhsoig](https://twitter.com/dhsoig).

## OIG HOTLINE

To expedite the reporting of alleged fraud, waste, abuse or mismanagement, or any other kinds of criminal or noncriminal misconduct relative to Department of Homeland Security (DHS) programs and operations, please visit our website at [www.oig.dhs.gov](http://www.oig.dhs.gov) and click on the red tab titled "Hotline" to report. You will be directed to complete and submit an automated DHS OIG Investigative Referral Submission Form. Submission through our website ensures that your complaint will be promptly received and reviewed by DHS OIG.

Should you be unable to access our website, you may submit your complaint in writing to:

Department of Homeland Security  
Office of Inspector General, Mail Stop 0305  
Attention: Office of Investigations Hotline  
245 Murray Drive, SW  
Washington, DC 20528-0305

You may also call 1(800) 323-8603 or fax the complaint directly to us at (202) 254-4297.

The OIG seeks to protect the identity of each writer and caller.