OFFICE OF INSPECTOR GENERAL

DHS Needs a Unified Strategy to Counter Disinformation Campaigns

Homeland Security

August 10, 2022

OIG-22-58

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Washington, DC 20528 / www.oig.dhs.gov

August 10, 2022

MEMORANDUM FOR: The Honorable Robert Silvers
Under Secretary
Office of Strategy, Policy, and Plans
Department of Homeland Security

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2022.08.09 16:41:11 -04'00'

SUBJECT: *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*

Attached is our final report, *DHS Needs a Unified Strategy to Counter Disinformation Campaigns.* We incorporated your formal comments into the final report.

The report contains one recommendation aimed at improving the Department's efforts to counter disinformation campaigns and efforts that appear in social media. The Department concurred with the recommendation. Based on information provided in the Department's response to the draft report, we consider this recommendation open and resolved. Once your office has fully implemented the recommendation, please submit a formal closeout letter to us within 30 days so that we may close the recommendation. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Please send your response or closure request to OIGAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act of 1978, as amended* we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the final report on our website for public dissemination.

Please call me with any questions, or your staff may contact Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG Highlights

DHS Needs a Unified Strategy to Disinformation Campaigns

August 10, 2022

Why We Did This Audit

In recent years, cyberattacks, intellectual property theft, and state-sponsored disinformation campaigns against our Nation have increased significantly. Our objective was to determine the internal and external coordination efforts the Department has taken to counter disinformation that appears in social media.

What We Recommend

We recommend DHS develop a unified strategy to counter disinformation campaigns that appear in social media.

For Further Information:
Contact our Office of Public Affairs at (202) 981-6000, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

The Department of Homeland Security began internal and external coordination efforts in 2018 to counter disinformation appearing in social media. These efforts were predominantly focused on disinformation campaigns that pertained to election infrastructure or to distinct mission operations.

Although DHS components have worked across various social media platforms to counter disinformation, DHS does not yet have a unified department-wide strategy to effectively counter disinformation that originates from both foreign and domestic sources. DHS faced challenges unifying component efforts because disinformation is an emerging and evolving threat. We also attributed some challenges to the continual changes in DHS leadership, which may have hindered the development of top-down strategic guidance for countering disinformation.

Without a unified strategy, DHS and its components cannot coordinate effectively, internally, or externally to counter disinformation campaigns that appear in social media.

DHS Response

The Department concurred with our recommendation. DHS management comments on a draft of this report are in Appendix A.

Background

A key Department of Homeland Security mission area is to secure cyberspace and critical infrastructure.[1] This mission has never been more important, as increased connectivity of people and devices to the internet and to each other has created an ever-expanding attack surface that extends throughout the world and into almost every American home.[2] Further, Americans increasingly rely on the internet and social media for news. To illustrate, in a 2021 survey, 93 percent of the adults sampled in the United States used the internet, as compared to 52 percent in 2000.[3] As more people rely on the internet for information, they become more vulnerable to manipulation, disinformation, and propaganda campaigns that appear in social media. False news, such as misinformation, disinformation, and malinformation[4] are used to shape public opinion, undermine trust, amplify division, and sow discord.[5]

Mobile devices and smartphones further enable individuals and groups to rapidly share content, including disinformation and misinformation. This content may include hyperlinks to media articles and other web-based content, such as images and videos,[6] that may have been manipulated to spread disinformation and misinformation, referred to as "deepfake" information.[7] Some deepfake videos are intended for entertainment, while others aim to use fake content to influence viewers to believe something happened that did not.

---

[1] DHS, *Strategic Planning*, last updated November 10, 2021, https://www.dhs.gov/strategic-planning.
[2] DHS, *Secure Cyberspace and Critical Infrastructure*, last updated February 23, 2022, https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure.
[3] Pew Research Center, *7 Percent of Americans don't use the internet. Who are they?,* April 2, 2021, https://www.pewresearch.org/fact-tank/2021/04/02/7-of-americans-dont-use-the-internet-who-are-they/.
[4] CISA defines disinformation as fabricated information intended to mislead or cause harm; misinformation is false, but not created or shared with the intention of causing harm; and malinformation is based on fact but used out of context to mislead, harm, or manipulate, https://www.cisa.gov/mdm.
[5] *CISA Insights, Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure*, February 2022, https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf.
[6] AEP 2019, *Combatting Targeted Disinformation Campaigns,* October 2019 https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.
[7] Merriam Webster defines a deepfake as an image or recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said, https://www.merriam-webster.com/dictionary/deepfake. According to the Regulatory Review, *Responding to Deepfakes and Disinformation*, August 14, 2021, deepfakes are uniquely effective at spreading disinformation, https://www.theregreview.org/2021/08/14/saturday-seminar-responding-deepfakes-disinformation/.

Some analysts have suggested deepfakes could be used to generate inflammatory content such as convincing video of U.S. military personnel engaged in war crimes intended to radicalize populations, recruit terrorists, or incite violence.[8] In 2019, an antivirus software company estimated more than 15,000 deepfake videos were being circulated on the internet.[9]

Attacks on organizations in critical infrastructure sectors have increased significantly during the past 10 years. To illustrate, there were fewer than 10 attacks in 2013 as compared to nearly 400 in 2020.[10] Further, a hostile nation engaged in state-sponsored malicious cyber activities, including espionage, intellectual property theft, disinformation, propaganda, and cyberattacks that targeted the United States.[11] For example, the SolarWinds cyber espionage campaign attempted to infiltrate Federal government networks in 2020.[12] In another example, during the 2016 U.S. presidential election campaign, foreign state-sponsored fake social media accounts were created to divide voters.[13]

Disinformation is manufactured information deliberately created or disseminated to mislead, harm, or manipulate a person, group, or country. A disinformation campaign occurs when a person, group of people, or entity (i.e., a "threat actor" or a hostile nation) coordinates to distribute false or misleading information while concealing the true objectives of the campaign.[14]

The objectives of disinformation campaigns can be broad (e.g., sowing discord in a population) or targeted (e.g., circulating a counternarrative to domestic protests). For example, such campaigns may aim to erode public trust in our government and the Nation's critical infrastructure sectors, negatively affect public discourse, or even sway elections. These campaigns can have foreign or domestic origins and may incorporate several different types of information

[8] Kelley M. Sayler and Laurie A. Harris, *Deepfakes and National Security*, June 8, 2021, https://crsreports.congress.gov/product/pdf/IF/IF11333.
[9] Forbes, *There Are Now 15,000 Deepfake Videos on Social Media. Yes, You Should Worry*, October 8, 2019, https://www.forbes.com/sites/johnbbrandon/2019/10/08/there-are-now-15000-deepfake-videos-on-social-media-yes-you-should-worry/?sh=75405acd3750.
[10] Katell Thielemann, *It's Time to Focus on Critical Infrastructure Systems Security,* January 24, 2022, https://www.cybersecuritydive.com/news/critical-infrastructure-security/617561/.
[11] *Senate Letter to DHS Regarding Efforts to Prevent Disinformation & Propaganda*, March 13, 2022, https://www.rosen.senate.gov/sites/default/files/2022-03/3290%20FINAL.pdf.
[12] CISA Alert (AA20-352A), *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organization*s, April 15, 2021, https://www.cisa.gov/uscert/ncas/alerts/aa20-352a.
[13] Gillian Cleary, *Twitter Bots: Anatomy of a Propaganda Campaign*, June 5, 2019, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/twitterbots-propaganda-disinformation.
[14]AEP 2019, *Combatting Targeted Disinformation Campaigns,* October 2019, https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

(disinformation, misinformation, propaganda, and true information). Specific examples of recent disinformation campaigns that targeted the United States include a foreign entity offering to pay social media influencers to criticize U.S. COVID-19 vaccines,[15] false claims of voter fraud during the November 2020 elections,[16] and bad actors using civil unrest as an opportunity to spread conspiracy theories and escalate tensions.[17]

According to a recent study on the evolving disinformation tactics used in social media in 2019 and 2020,[18] false or misleading information presented as news remains a popular tactic for disinformation. Both Facebook and Twitter often removed pages or accounts that pretended to be independent news outlets. Certain countries were far more likely than others to be targeted by foreign disinformation operations. Based on publicly available information from Facebook and Twitter, the three countries most targeted by foreign actors were the United States, the United Kingdom, and Egypt. Fake accounts that include a profile photo appear more authentic and convincing. Bad actors sometimes use profile pictures that are automatically generated by artificial intelligence; because these pictures are not of actual humans, bad actors can evade reverse image searching or detection.[19]

According to Presidential Policy Directive 41, *United States Cyber Incident Coordination*, dated July 2016,[20] DHS is responsible for coordinating the national response to cyber incidents. Several components play key roles in this effort. Primarily,

- the Cybersecurity and Infrastructure Security Agency (CISA) fulfills DHS' cybersecurity mission and leads the national effort to understand, manage, and reduce risk to cyber and physical infrastructure; and

- the Office of Intelligence and Analysis (I&A) provides the Department with the intelligence and information it needs to keep the country safe, secure, and resilient. I&A also works closely with other components'

[15] WTOP, *COVID Conspiracy: Foreign Disinformation Driving American Vaccine Resistance*, September 27, 2021, https://wtop.com/j-j-green-national/2021/09/covid-conspiracy-foreign-disinformation-driving-american-vaccine-resistance/.
[16] PEW, *Election Disinformation Fears Came True for State Officials*, November 20, 2020, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/11/20/election-disinformation-fears-came-true-for-state-officials.
[17] Christina Georgapoulos and Trey Poche, *Fake news, disinformation and the George Floyd Protests*, August 2020, https://faculty.lsu.edu/fakenews/about/protestfakenews.php.
[18] Brookings, *How Disinformation Evolved in 2020*, January 4, 2021, https://www.brookings.edu/techstream/how-disinformation-evolved-in-2020/.
[19] *Id.*
[20] Presidential Policy Directive 41, *United States Cyber Incident Coordination,* July 26, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

> intelligence elements, as well as state, local, tribal, and private sector entities, to combine nontraditional streams of information with traditional intelligence community sources and provide a complete assessment of threats to the Nation.

We conducted this audit to determine the internal and external coordination efforts the Department has taken to counter disinformation campaigns and efforts that appear in social media.

Results of Audit

During the past few years, some DHS components have taken actions to counter disinformation campaigns that either pertained to the election infrastructure or distinct mission areas. However, as disinformation represents an emerging and evolving threat, DHS does not yet have a unified strategy or top-down guidance from the Secretary to mitigate disinformation. Without a more unified approach, DHS cannot effectively mitigate emerging threats or unify its work to counter disinformation campaigns that appear in social media from both foreign and domestic sources.

DHS Components Have Made Efforts to Counter Disinformation

As part of its overarching effort to improve our Nation's cybersecurity, several DHS components have conducted work to counter disinformation and build awareness. To date, these efforts have been predominantly focused on disinformation campaigns that pertained to election infrastructure or to distinct DHS mission operations. We conducted an overarching review of these disinformation campaigns, noting that CISA and I&A primarily led the Department's efforts focused on election security leading up to the 2020 elections.

First, in 2018, former DHS Secretary Kirstjen Nielsen established the Countering Foreign Influence Task Force (Task Force) to focus on election infrastructure disinformation. The Task Force comprised CISA's Election Security Initiative division and I&A staff. From 2018 to 2021, the Task Force developed threat intelligence and engaged with stakeholders related to elections. According to CISA's website and an internal document, in 2018, CISA also started notifying social media platforms or appropriate law enforcement officials when voting-related disinformation appeared in social media.[21] Once CISA notified a social media platform of disinformation, the social media platform could independently decide whether to remove or

[21] CISA's MDM website, accessed July 13, 2021, states it continues to make social media platforms and law enforcement aware of disinformation, https://www.cisa.gov/mdm.

modify the post.[22]

Next, according to an I&A official, as part of the Department's election security efforts, I&A created a Foreign Influence and Interference Branch in 2019, to organize and create analytical products about disinformation. In this role, the Foreign Influence Branch did not directly counter disinformation; but rather, it shared information on the current threat environment. This information is shared through intelligence briefs and reference aids on foreign adversaries, among other methods. The I&A official stated that the Foreign Influence Branch has 15 staff dedicated to creating analytical products about disinformation. The Department's Office for Civil Rights and Civil Liberties (CRCL) also helped I&A with its election efforts starting in 2016. CRCL reviewed I&A's disinformation-related intelligence products and determined that these products did not violate U.S. citizens' civil rights.

During the same period, CISA began issuing web-based materials to build awareness about disinformation campaigns. This work was directly aligned to the Department's 2019 strategy[23] to outline various initiatives to mitigate threats, including disinformation. In this document, DHS pledged to develop media/information literacy toolkits to raise awareness of disinformation campaigns targeting communities in the United States. In accordance with this framework, CISA released numerous web-based materials to educate the public about disinformation campaigns and tactics. CISA's original material focused on election-related disinformation and tactics used by those spreading mis-, dis-, and malinformation (MDM) generally, and subsequently expanded to include other areas related to COVID-19 and vaccines. Examples of these materials include:

- The *Resilience Series* – two web-based graphic novels[24] that used sequential art to tell a short story to help individuals understand the risks foreign influence operations pose. The graphics in the novels are meant to highlight the importance of evaluating information sources.

[22] CISA's email correspondence to Social Media platforms included the following disclaimer: "*The Cybersecurity and Infrastructure Security Agency (CISA) of the U.S. Department of Homeland Security (DHS) is not the originator of this information. CISA is forwarding this information, unedited, from its originating source – this information has not been originated or generated by CISA. This information may also be shared with law enforcement or intelligence agencies. CISA affirms that it neither has nor seeks the ability to remove or edit what information is made available on social media platforms. CISA makes no recommendations about how the information it is sharing should be handled or used by social media companies. Additionally, CISA will not take any action, favorable or unfavorable, toward social media companies based on decisions about how or whether to use this information.*"
[23] *Strategic Framework for Countering Terrorism and Targeted Violence,* 2019.
[24] CISA's *Bug Bytes* graphic novel, accessed April 29, 2021, https://www.cisa.gov/resilience-series-graphic-novels.

Figure 1 is an image from the *Real Fake* graphic novel in CISA's *Resilience Series*.

Figure 1. *Real Fake* Graphic Novel

Source: CISA's *Real Fake* graphic novel[25]

- The *#Protect2020 Rumor vs. Reality* – a web page[26] dedicated to debunking common misinformation and disinformation narratives and themes that related broadly to the 2020 elections and the security of the election infrastructure. The website includes sections on understanding foreign influence and enhancing election infrastructure resiliency.

- The *Tools of Disinformation: Inauthentic Content* – an online factsheet[27] to outline how disinformation actors use a variety of tools (e.g., deepfakes, forged artifacts, and proxy sites)[28] to influence their victims.

More recently, in January 2021, CISA transitioned its Countering Foreign Influence Task Force to promote more flexibility to focus on general MDM. A CISA official stated that the component established an MDM team with a total of 15 dedicated part- and full-time staff. The MDM team focuses on disinformation activities targeting elections and critical infrastructure. According to a CISA official, the MDM team counters all types of disinformation, to be responsive to current events. For example, the MDM team developed the *COVID-19 Disinformation Toolkit*[29] to raise awareness related to the pandemic. In April 2022, the MDM team released the *Social*

[25] CISA's *Real Fake* graphic novel, accessed April 29, 2021, https://www.cisa.gov/resilience-series-graphic-novels.
[26] CISA, #Protect2020 webpage, accessed April 29, 2021, https://www.cisa.gov/protect2020.
[27] CISA, *Tools of Disinformation: Inauthentic Content*, accessed April 29, 2021, https://www.cisa.gov/sites/default/files/publications/mdm-inauthentic-content-product-english_508.pdf.
[28] CISA's factsheet states that forged artifacts typically feature fake letterheads, copied and pasted signatures, made-up social media posts, and maliciously edited emails. Proxy websites are fronts for malicious actors, designed to launder disinformation and divisive content or use that content to drive website visits, accessed May 11, 2021, https://www.cisa.gov/sites/default/files/publications/mdm-inauthentic-content-product-english_508.pdf.
[29] *COVID-19 Disinformation Toolkit,* accessed April 29, 2021, https://www.cisa.gov/covid-19-disinformation-toolkit.

Media Bots Infographic Set[30] designed to help Americans understand how automated programs simulate human behavior on social media platforms. The infographic set also illustrates how bad actors use social media bots to spread false or misleading information, shut down opposition, and elevate their own platforms for further manipulation. An official from the MDM team stated that, through this work, CISA is building national resilience to MDM, such as COVID-19 vaccine hesitancy and foreign influence activities. CISA continues to address MDM threats through web-based materials educating the public on disinformation campaigns initiated by both foreign and domestic sources on topics, such as 5G communications technology and the risk to the Nation.

We also identified several component-led efforts that span the last 3 years to counter disinformation originating from foreign and domestic sources. For the most part, these efforts centered around each component's distinct mission area by directly contacting the media or conducting mission-focused work. According to DHS component officials, these efforts include:

- U.S. Customs and Border Protection – the Digital Engagement Office determines whether information about the component spread through social media platforms like Facebook and Twitter is accurate.

- U.S. Immigration and Customs Enforcement – the Homeland Security Investigations' Public Affairs Office issues press releases in response to disinformation about the work conducted by Homeland Security Investigations.

- Science and Technology Directorate – the directorate researches how humans use and consume disinformation from a behavioral perspective. The directorate's research included determining whether social media accounts were bots or humans and how the mayhem caused by bots affects behavior.

- United States Secret Service – an official stated that it had contacted the media in 2021 to correct information related to a person the United States Secret Service protects.

- The Department's Center for Prevention Programs and Partnerships – provides resources to community organizations and other Department stakeholders to promote digital literacy and build resilience to disinformation.

[30] *Social Media Bots Infographic Set,* accessed May 11, 2021, https://www.cisa.gov/sites/default/files/publications/social_media_bots_infographic_set_508.pdf.

Based on a list of contacts a CISA official provided, the component works with members of the intelligence community to counter disinformation campaigns that appear on social media. According to selected Intelligence Community officials, the Office of the Director of National Intelligence and the U.S. Department of Justice worked with CISA and I&A to counter disinformation related to the November 2020 elections. For example, according to an Office of the Director of National Intelligence official, prior to the November 2020 elections, CISA and I&A joined in weekly teleconferences to coordinate Intelligence Community activities to counter election-related disinformation. The Office of the Director of National Intelligence official stated the teleconferences continued to occur every 2 weeks after the 2020 elections and were still taking place as of the time of this audit.

CISA and I&A also work with the U.S. Department of State's (State Department) Global Engagement Center on countering disinformation. According to a State Department official, when the Global Engagement Center identifies disinformation campaigns abroad, it shares its analysis and reports with CISA and I&A to improve DHS' understanding of adversarial tactics, techniques, and procedures in spreading disinformation. The official added that another joint effort between CISA and the State Department involved working on Harmony Square, an online game that teaches players to recognize disinformation.

DHS Does Not Have a Department-wide Strategy to Counter Disinformation that Appears in Social Media

Although many component initiatives are underway, the Department has not taken a holistic approach to effectively counter disinformation from foreign and domestic sources. According to Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, dated February 2013,[31] the Secretary of Homeland Security is required to provide strategic guidance and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure. However, DHS does not have a unified, department-wide strategy to set overarching goals and objectives for addressing and mitigating threats from disinformation campaigns that appear in social media. Absent a central strategy for use department-wide, DHS components' efforts were directed by the following guidance documents related to election security:

- In September 2019, former Acting Secretary Kevin McAleenan issued *DHS Strategic Framework for Countering Terrorism and Targeted*

[31] Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience,* February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Violence.[32] This document highlighted the shift in how U.S. citizens access information and the threats disinformation poses. Specifically, it detailed bad actors' efforts to use disinformation campaigns to capitalize on American political divisions and increase strife and division. Goal 3, "Prevent Terrorism and Targeted Violence," focused on countering disinformation from foreign influence operations.

- In October 2020, former Acting Secretary Chad Wolf issued the *Homeland Threat Assessment*,[33] which highlighted cyber threats to critical infrastructure and the U.S. democratic process from bad actors. The *Homeland Threat Assessment* also explained tactics that foreign actors may use to inflame narratives about the COVID-19 pandemic and amplify U.S. socio-political division.

Because each component has different limitations to its authorities, the components cannot address the full range of potential threats from disinformation. A department-wide strategy would assist in addressing these limitations. Based on feedback from our interviews and a review of requested guidance, the Department and its components have the following limitations to their authorities:

- CISA can only counter disinformation that represents a threat to critical infrastructure security and cybersecurity.

- CISA must protect U.S. citizens' privacy and cannot collect and share disinformation from social media posts if it results in disadvantages to people with a particular viewpoint or involves personally identifiable information.

- CISA and I&A must consider a U.S. citizen's First Amendment right to free speech in social media and the rights of the readers of posts.

A DHS-wide strategy can also promote consistency across the Department as components address privacy, constitutional, and other legal issues. The absence of a unified department-wide strategy has also led to confusion by external partners regarding specific DHS components' responsibilities and whom to contact within DHS. During interviews with members of the Intelligence Community, we learned that officials at the Office of the Director of

[32] *DHS Strategic Framework for Countering Terrorism and Targeted Violence,* September 2019, https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.
[33] *Homeland Threat Assessment,* October 2020, https://www.dhs.gov/sites/default/files/publications/2020_10_06_homeland-threat-assessment.pdf.

National Intelligence have expressed concerns about whether CISA or I&A is the lead component for countering disinformation. Members of the Intelligence Community also questioned the effectiveness of components' ongoing efforts. For example, an Intelligence Community official voiced concerns about whether CISA's myth-busting website was doing enough to effectively counter disinformation.

DHS faces several challenges that hinder its ability to develop a unified strategy to mitigate disinformation campaigns in social media. First, the disinformation tactics that are being used on social media are constantly evolving and becoming an urgent emerging threat to our Nation. As more people rely on the internet for information, they become more prone to manipulation, disinformation, and propaganda campaigns when skepticism is not exercised to question the authenticity and validity of the source of information. The Department has highlighted this transition in how U.S. citizens access information and the threats from disinformation in the 2019 *Strategic Framework for Countering Terrorism and Targeted Violence*.[34]

Second, continual changes in DHS leadership have made it less likely for this emerging area to be a strategic, high-level focus. The current DHS Secretary[35] was the first confirmed Secretary of Homeland Security in nearly 2 years since April 2019. In the interim, DHS had four Acting Secretaries. Although a confirmed Secretary is now in place, DHS components reportedly are waiting for direction pertaining to countering disinformation. To illustrate, according to an official, CISA would not make any major change in how it counters disinformation until it receives guidance from new leadership.

In January 2022, an Office of the General Counsel official said the DHS Secretary is reviewing ongoing work focused on countering disinformation but has not yet decided on a department-wide strategy.[36] Without DHS senior leadership guidance as a foundation, components cannot work successfully to counter disinformation campaigns originating from both foreign and domestic sources.

---

[34] *Strategic Framework for Countering Terrorism and Targeted Violence,* September 2019, https://www.dhs.gov/sites/default/files/publications/19_0920_plcy_strategic-framework-countering-terrorism-targeted-violence.pdf.

[35] Alejandro Mayorkas was sworn in as DHS Secretary on February 1, 2021.

[36] In an April 2022 House Judiciary Committee hearing, the DHS Secretary stated that the Department had established a Disinformation Governance Board to focus on the dissemination of disinformation. Three weeks after DHS Secretary's announcement, it was reported that the Department decided to "pause" the Disinformation Governance Board and its work. We did not validate detailed information about the board, a strategy, or milestones as part of this audit, as it was formed after our fieldwork was complete. Washington Post, *How the Biden administration let right-wing attacks derail its disinformation efforts*, May 18, 2022, https://www.washingtonpost.com/technology/2022/05/18/disinformation-board-dhs-nina-jankowicz/.

Conclusion

According to the DHS *Strategic Framework for Countering Terrorism and Targeted Violence*, disinformation campaigns aim to shape public opinion or undermine trust which may foment strife and division. This emerging threat continues to evolve as Americans increasingly rely on social media for news and bad actors develop new tactics to sow discord. Although DHS is responsible for coordinating the national response to cyber incidents, the Department has yet to develop a unified strategy to counter disinformation. Without a unified strategy, DHS faces limited communication and awareness among its components, restrictions, and confusion over which DHS component should lead specific efforts to counter disinformation. A more unified strategy is also needed to mitigate the threat of civil unrest from disinformation that may spread rumors about COVID-19 vaccines or increase fear about food and supply shortages, among other things.

Recommendation

We recommend the Office of Strategy, Policy, and Plans develop a unified strategy to improve DHS' coordinated actions among the components and with other agencies to counter disinformation campaigns that appear in social media.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Under Secretary, Office of Strategy, Policy, and Plans, who expressed the Department's appreciation for OIG's work in planning and conducting its review and issuing this report. A copy of DHS' response in its entirety is in Appendix A. DHS also provided technical comments and suggested revisions to our report in a separate document. We reviewed the technical comments and made changes to the report where appropriate.

Response to Report Recommendation

The Department concurred with our recommendation. Following is a summary of DHS' response to the recommendation and the OIG's analysis.

DHS Comments to Recommendation: Concur. In May 2022, Secretary Mayorkas asked the bipartisan Homeland Security Advisory Council (HSAC) to review the Department's work on addressing disinformation that threatens homeland security. The Department plans to share with the public HSAC's final recommendations, which are expected to be completed in August 2022. DHS leadership will determine its strategic direction on countering disinformation after reviewing these recommendations and consulting with

stakeholders, including congressional members, as appropriate. Estimated Completion Date: August 31, 2023.

OIG Analysis of DHS Comments: DHS' actions are responsive to this recommendation, which will remain open and resolved until DHS provides documentation showing that all planned corrective actions are completed.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296) by amendment to the *Inspector General Act of 1978*.

Our objective was to determine the internal and external coordination efforts the Department has taken to counter disinformation campaigns and efforts that appear in social media.

Our audit focused on the requirements, recommendations, and goals outlined in the following key documents:

- Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience,* February 2013;
- Presidential Policy Directive 41, *United States Cyber Incident Coordination*, dated July 2016;
- DHS *Strategic Framework for Countering Terrorism and Targeted Violence*, September 2019; and
- DHS *Homeland Threat Assessment*, October 2020.

To conduct our audit, we interviewed selected personnel from CISA; I&A; U.S. Immigration and Customs Enforcement; Office for Civil Rights and Civil Liberties; Office of Strategy, Policy, and Plans; Office of Targeted Violence and Terrorism Prevention; Science and Technology Directorate; the United States Secret Service; and U.S. Customs and Border Protection concerning the coordination efforts the Department has taken to counter disinformation campaigns that appear in social media.

In addition, we met with personnel from the following organizations to obtain their perspectives on DHS' efforts to counter disinformation:

- Office of the Director of National Intelligence;
- U.S. Department of Justice; and
- DOS Global Engagement Center.

As part of our review, we assessed the internal and external coordination

efforts the Department has taken to counter disinformation in social media. Because we did not obtain any computer-processed data related to disinformation, we did not conduct any data reliability tests.

We conducted this audit between January 2021 and February 2022 pursuant to the *Inspector General Act of 1978, as amended,* and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objective.

The Office of Audits major contributors to this report are Chiu-Tong Tsang, Audit Director; Marcie McIsaac, Audit Manager; Barry Bruner, Auditor-in-Charge; Omar Russell, Auditor-in-Charge; Stuart Josephs, Auditor; and Maria Romstedt, Communications Analyst.

Appendix A
DHS Comments to the Draft Report

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

Homeland Security

July 15, 2022

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Robert Silvers
Under Secretary
Office of Strategy, Policy, and Plans

SUBJECT: **Management Response to Draft Report: "DHS Needs a Unified Strategy to Counter Disinformation Campaigns" (Project No. 21-015-AUD-CISA)**

Thank you for the opportunity to comment on the draft report entitled "DHS Needs a Unified Strategy to Counter Disinformation Campaigns" (report). The Department of Homeland Security's (DHS or the Department) Office of Strategy, Policy, and Plans (PLCY) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS leadership appreciates OIG's acknowledgement of DHS's role in safeguarding the United States against threats to its security, including those exacerbated by disinformation. As part of its mission, DHS has worked for nearly 10 years across multiple administrations to address disinformation that threatens our homeland security and the security of the American people. This includes (1) U.S. Customs and Border Protection's efforts to counter disinformation spread by cartels and human smugglers to persuade migrants to cross our southwest border illegally; (2) efforts by the Federal Emergency Management Agency to correct false information spread in the wake of natural disasters and other national emergencies, including to ensure that this false information does not prevent Americans from accessing federal aid during and after disasters and to prevent them from becoming victims of fraud; and (3) the Cybersecurity and Infrastructure Security Agency's work with stakeholders to mitigate the risk of disinformation that threatens critical infrastructure.

This work is conducted by DHS component agencies pursuant to their respective authorities and consistent with privacy, civil rights, and civil liberties safeguards, as well as other applicable laws. The Department's Office of the General Counsel, Office of Civil Rights and Civil Liberties, PLCY, and Privacy Office exercise their statutory

1

responsibilities to ensure disinformation-related work within relevant DHS component agencies, like all of the Department's work, is conducted lawfully, pursuant to appropriate safeguards, and in a manner that honors and upholds our nation's values.

The draft report contained one recommendation, with which PLCY concurs. Enclosed is a more detailed response to the recommendation. PLCY previously submitted under separate cover extensive technical comments addressing several accuracy, contextual, and other issues for OIG's consideration. We look forward to receiving your adjudication of these comments.

Thank you again for the opportunity to review and comment on this draft report. Please contact me if you have any questions.

Enclosure

Enclosure: Management Response to Recommendations Contained in 21-015-AUD-CISA

OIG recommended that the Under Secretary for PLCY:

Recommendation 1: Develop a unified strategy to improve DHS's coordinated actions among the Components and with other agencies to counter disinformation campaigns that appear in social media.

Response: Concur, subject to the Department's consideration of the ongoing review Secretary of Homeland Security Alejandro N. Mayorkas asked the bipartisan Homeland Security Advisory Council (HSAC) to conduct in May 2022 of the Department's work to address disinformation that threatens homeland security, with a focus on two pivotal areas:

(1) how the Department can most effectively and appropriately address disinformation that poses a threat to our country while protecting free speech, privacy, civil rights, and civil liberties; and,

(2) how DHS can achieve greater transparency across its disinformation-related work and increase trust with the public and other key stakeholders.

The HSAC's final recommendations, which are expected to be completed in August 2022, will be shared with the public. DHS leadership will determine its strategic direction on countering disinformation after reviewing these recommendations and consulting with key stakeholders, including members of Congress, as appropriate.

Estimated Completion Date: August 31, 2023.

3

Appendix B
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, or write to us at:

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