



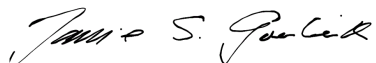
# Homeland Security Advisory Council

Disinformation Best Practices and Safeguards Subcommittee

Final Report

August 24, 2022

This publication is presented on behalf of the Homeland Security Advisory Council, Homeland Security Advisory Council (HSAC) Subcommittee for Disinformation Best Practices and Safeguards, Co-Chaired by Jamie Gorelick and Michael Chertoff to the Secretary of the Department of Homeland Security, Alejandro N. Mayorkas.



---

Jamie Gorelick, Co-Chair  
Partner  
WilmerHale



---

Michael Chertoff, Co-Chair  
Co-Founder and Executive Chairman  
The Chertoff Group

This page is intentionally left blank.

## **TABLE OF CONTENTS**

---

SUBCOMMITTEE FOR DISINFORMATION BEST PRACTICES AND SAFEGUARDS	5
HOMELAND SECURITY ADVISORY COUNCIL STAFF	5
INTRODUCTION	6
DEFINITIONS	6
IMPACT ON MISSIONS	6
DHS ACTIVITIES	8
RECOMMENDATIONS	12
APPENDIX 1: EXAMPLES OF DISINFORMATION IMPAIRING DHS’S CORE MISSIONS AND EXAMPLES OF PRODUCTS RELEASED	17
APPENDIX 2: COMPILATION OF PRODUCTS (PROVIDED IN SEPARATE DOCUMENT)	23
APPENDIX 3: TASKING LETTER	24
APPENDIX 4: SUBCOMMITTEE MEMBER BIOGRAPHIES	26
APPENDIX 5: SUBJECT MATTER EXPERTS AND OTHER WITNESSES	29

**SUBCOMMITTEE FOR DISINFORMATION BEST PRACTICES AND SAFEGUARDS**

**Jamie Gorelick, Co-Chair**

**Partner  
WilmerHale**

**Michael Chertoff, Co-Chair**

**Co-Founder and Executive Chairman  
The Chertoff Group**

**Ted Schlein**

**General Partner, Kleiner Perkins  
Executive Chairman, Ballistic Ventures**

**Sonal Shah**

**Executive Vice President, United Way Worldwide  
Founding President, The Asian American Foundation**

**Ali Soufan**

**Chairman and CEO  
The Soufan Group**

**Matthew F. Ferraro**

**Counsel  
WilmerHale**

**HOMELAND SECURITY ADVISORY COUNCIL STAFF**

<b>Jason Mayer</b>	<b>Designated Federal Official</b>
<b>Rebecca Sternhell</b>	<b>Executive Director Homeland Security Advisory Council</b>
<b>Mike Miron</b>	<b>Deputy Executive Director Homeland Security Advisory Council</b>
<b>Alexander Jacobs</b>	<b>Senior Director Homeland Security Advisory Council</b>
<b>Joseph Chilbert</b>	<b>Senior Director Homeland Security Advisory Council</b>

## INTRODUCTION

---

On May 18, 2022, Secretary Mayorkas asked a Subcommittee of the Department of Homeland Security’s Homeland Security Advisory Council to make recommendations for how the Department can most effectively and appropriately address disinformation that poses a threat to the homeland while protecting civil rights and providing greater transparency across this work.

This report presents our assessment and recommendations. Part I defines our terms. Part II provides concrete examples of disinformation’s deleterious impacts on DHS’s Congressionally mandated missions. Part III describes DHS’s current activities. Part IV contains our recommendations. Our review preceded the release by the DHS Inspector General (IG) of its report, “DHS Needs a Unified Strategy to Counter Disinformation Campaigns,” but many of the observations in that report are consistent with our own. Our recommendations would produce a more strategic approach to disinformation.<sup>1</sup>

## DEFINITIONS

---

We begin with a brief discussion of the definitions we used in this review.

Disinformation is, in essence, a particularly pernicious form of inaccurate information. As the Inspector General observed, 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.”<sup>2</sup> Disinformation has three variants: Disinformation is the deliberate dissemination of falsehoods. Misinformation is the unintentional propagation of falsehoods. Malinformation is the intentional spreading of genuine information with the intent to cause harm, for example, by moving private and personal information into the public sphere.<sup>3</sup> For ease of use, this report employs the term “disinformation” to refer broadly to all of these variants. While lies and gossip are ancient vices, changes in telecommunications and social media permit disinformation to spread at an unprecedented scale, speed, and scope. Images and other forms of media can be forged to look real, making it difficult for individuals and organizations to know what is true and what is false.

---

<sup>1</sup> The IG recommended that DHS “develop a unified strategy to counter disinformation campaigns that appear in social media.” *DHS Needs a Unified Strategy to Counter Disinformation Campaigns*, No. OIG-22-58, DHS Inspector General (Aug. 10, 2022) <https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf> (hereinafter: “IG Report”).

<sup>2</sup> *Id.* at 3.

<sup>3</sup> These definitions are consistent with those used by the Cybersecurity and Infrastructure Security Agency (CISA). *See Mis, Dis, Malinformation*, CISA, <https://www.cisa.gov/mdm>.

## IMPACT ON MISSIONS

---

Congress created the Department to fulfill important national missions, including countering terrorism and threats to the security of the country, securing our borders, protecting the nation's cybersecurity and critical infrastructure (including election infrastructure), and providing rapid and effective responses to natural disasters, among others. Its authorities are grounded in the statutes creating each of its components.<sup>4</sup>

The spread of disinformation poses threats to these missions, as shown by the below examples and in Appendix 1. Examples are grouped by the DHS components responsible for the relevant DHS mission.

### *Cybersecurity and Infrastructure Security Agency*

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.<sup>5</sup> There are many examples of the types of disinformation with which it must deal.

**Critical Infrastructure:** The spread of disinformation has led to material threats to critical infrastructure targeting public health, communications, financial services, the defense industrial base, and rare-earth mineral producers, which are critical to U.S. security. These threats impact the operations of critical infrastructure, their finances, and reputations. For example, in the early summer of 2020, a conspiracy spread widely online that 5G cell towers are responsible for the spread of the coronavirus, leading to attacks on cell phone towers and telecommunications workers, particularly in the United Kingdom, continental Europe, and New Zealand. As a result, DHS issued an advisory to the U.S. telecommunications industry that the dangers of coronavirus conspiracists inciting attacks against communications infrastructure would probably increase as the disease spread.<sup>6</sup>

**Election Security:** Disinformation undermines confidence in the security of U.S. elections. False statements on this topic have had significant operational impacts on U.S. elections and election offices through increased threats to election workers, which has led to increased attrition of election workers.

### *U.S. Customs and Border Protection*

U.S. Customs and Border Protection (CBP) is responsible for protecting our borders. It has a strong interest in responding to false statements by human smugglers that threaten border security. To lure migrants to the border, smugglers have spread false statements that anyone

---

<sup>4</sup> See generally Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135 (2002).

<sup>5</sup> See IG Report at 4.

<sup>6</sup> See Josh Margolin, *Feds Warn of Attacks Related to Bogus COVID-19 Conspiracy Theory*, ABC NEWS (May 16, 2020, 12:04 PM), <https://abcnews.go.com/US/feds-warn-attacks-related-bogus-covid-19-conspiracy/story?id=70721145>.

smuggled into the United States receives asylum and that pregnant women will be allowed into the country. CBP has seen many examples of smugglers' ads on social media and in chat rooms in Spanish and English claiming they can get migrants safely into the United States for a price. Ads also offer counterfeit identification documents and target specific nationalities or groups. This disinformation drives migration to the United States, endangers the lives of migrants, and undermines the Department's mission to secure the nation's borders.

#### *The Federal Emergency Management Agency*

The Federal Emergency Management Agency (FEMA) is required to prepare for and respond to natural and other disasters. It has seen how disinformation has targeted victims of natural disasters. For example, FEMA has observed a rise in disinformation targeting individuals via text or direct messaging, telling them to send their bank account information to a particular address or website in order to receive FEMA assistance. These scams allow bad actors to compromise the victims' bank accounts. The agency has also tracked the spread of false rumors that FEMA is giving out gift cards or that FEMA is picking up debris from private property. These myths negatively impact FEMA's mission.

False narratives can also lead to offline actions that threaten the safety and security of responder personnel and/or disaster survivors, cause operational disruptions that impede disaster response and recovery efforts, and diminish public trust and confidence in the agency.

#### *United States Secret Service*

Disinformation has the potential to impact both the individuals protected by the United States Secret Service (Secret Service) and the overall effectiveness of the agency. The Secret Service is aware that disinformation has the potential to impact its protective mission. For example, malicious entities could post disinformation on social media platforms that could resonate with radical or malicious groups, causing them to disrupt the security plan of a protected site or threaten a protectee.

## **DHS ACTIVITIES**

---

This section reviews DHS's activities to detect the spread of narratives potentially harmful to DHS's missions and what it does to mitigate those harms.

### **a. Detection**

DHS components vary in how they track the dissemination of disinformation that can undermine core Departmental missions.

#### *Cybersecurity and Infrastructure Security Agency*

CISA's National Risk Management Center (NRMC) reviews public reporting from third parties,



both inside the Federal government (*e.g.*, DHS's Office of Intelligence and Analysis and the Department of State's Global Engagement Center) and outside the government, on the spread of viral narratives. The reporting it receives from outside the government is publicly available. The NRMC does not have the operational capability to track or identify disinformation campaigns itself.

#### *Office of Intelligence and Analysis*

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.<sup>7</sup> I&A identifies the spread of disinformation through all-source intelligence research, including open-source collection from known forums (*e.g.*, attributed foreign-operated social media accounts, attributed foreign-operated proxy websites, state-controlled media), to establish narratives, tactics, techniques, and procedures used by known foreign actors and domestic violent extremists. These intelligence activities result in Open Source Information Reports (OSIRs), Intelligence Information Reports (IIRs), and various forms of finished intelligence that can be read by I&A's partners in the U.S. government, as well as by state, local, tribal, and territorial (SLTT) institutions, and others, when appropriate.

#### *Federal Emergency Management Agency*

FEMA identifies rumors by leveraging a team in its Office of External Affairs to conduct searches on social media for public conversations. That team analyzes the information to support situational awareness during disaster responses. In some cases, FEMA also receives reports from federal partners, like CISA and the Department of State. In late 2020, FEMA began a preparedness training initiative for members of the SLTT emergency management community designed to increase knowledge and understanding of the online information space to include the real and potential risks associated with rumors that may propagate during disasters and emergencies. FEMA also uses an agreement with the Department of Energy's Argonne National Laboratory Federally funded Research and Development Center to assist with the analysis of data on viral narratives.

#### *United States Secret Service*

The Secret Service receives disinformation-tracking information from other DHS components as well as other federal and state agencies. The Secret Service's Open Source Branch (OSB) does not search for disinformation or purchase technical tools for that purpose. OSB analysts are trained to spot potential fake (or bot) accounts for the purpose of identifying investigative leads for threatening statements. While the agency does not specifically seek out disinformation, it nevertheless observes in the ordinary course of its duties what are likely fake social media accounts that could serve to deliver disinformation.

#### *U.S. Customs and Border Protection*

CBP uses software to search, find, and track the spread of online messages and attitudes related

---

<sup>7</sup> IG Report at 4.

to migration. CBP shares and receives information on disinformation with CISA, FEMA, the U.S. Department of Defense, and the Department of State.

**b. Mitigation**

DHS components currently engage in a number of activities to address the disinformation that impairs its core missions. These activities focus on the following:

*Identifying information on disinformation threats and trends in order to assess their risks to homeland security.*

As noted above, many components seek to identify disinformation that can undermine DHS missions. For example, I&A shares intelligence analysis to help identify and mitigate threats to the homeland. Its focus is to provide the Department with both the tactical intelligence and strategic analysis to keep the homeland safe, secure, and resilient. It provides public information about disinformation threat streams, and it helps other Departmental components and other government entities understand those threats. I&A's Cyber Mission Center collects information on foreign malign influence activity, analyzing both official traditional and social media channels backed by foreign states and proxy websites and forums. And I&A's Current and Emerging Threats Center and Counterterrorism Mission Center collect open-source information on the threats of domestic violent extremists (DVE). This collection may surface disinformation narratives or trends associated with identified DVE threat actors.

Other DHS components identify disinformation that impacts their specific authorized missions. FEMA takes note of information online that interferes with FEMA's ability to deliver public assistance in the wake of major disasters, and CBP attends to narratives that enable human trafficking and smuggling.

*Informing federal, state, local, tribal and territorial government institutions, non-governmental entities and, where appropriate, the public about disinformation that threatens the homeland.*

DHS components share with other agencies and non-governmental entities information about threats to our homeland security. For example, CISA and I&A coordinate with interagency partners including the FBI and the rest of the Intelligence Community to share information on election security threats, supporting an interagency notification framework. CISA also shares information with key non-governmental entities about disinformation threats to election integrity and election security. CBP works to understand the ways in which human smugglers are using platforms and messaging tools to deceive individuals and encourage them to make a dangerous journey to our borders. Public advisories, such as National Terrorism Advisory System (NTAS) bulletins issued by DHS, reference the threat of disinformation spread by both foreign malign-influence actors and domestic violent extremism threat actors.

*Responding to clearly erroneous assertions of basic facts when they pose threats to security of the homeland.*

DHS often responds to dangerous and false narratives in its areas of operation by simply

providing accurate information to the public. For example, CISA’s “Rumor Control” website addresses false rumors about election security. It has issued statements about the rumor that voting system software is not reviewed or tested and can easily be manipulated. It has posted accurate information in response to the falsehood that poll workers in the 2020 elections were giving certain writing instruments, like Sharpies, to specific voters in order to cause their ballots to be rejected. Where CISA finds information that is relevant to how state and local election officials protect elections, it passes that information on to them either directly or through an entity called an Information Sharing and Analysis Center, a non-profit, member-driven organization formed by critical infrastructure owners and operators to share information between government and industry. When CISA receives information from state and local election officials on disinformation campaigns utilizing social media, CISA passes that information to the social media companies for whatever action those companies see fit to take.

With regard to public health, during the height of the pandemic, CISA also posted public information about COVID-19, its origin and scale, the government’s response, and proper prevention and treatment. For example, a CISA “Insight” from May 2020 corrected disinformation then circulating that the National Guard Bureau would be called out to enforce nationwide quarantines. (For this and other examples of products released by DHS components to address disinformation, see Appendix 2.)

Likewise, CBP has sought to respond to false statements by human smugglers that can prompt illegal migration through a “Say No to the Coyote” campaign and other media campaigns in Central America to spread accurate information about our immigration system.

FEMA, through its public affairs channels, has drawn attention to scams that trick victims into providing malefactors with their bank account information under the guise of seeking disaster aid. FEMA has responded by providing authoritative information on how disaster victims can access assistance. Also, during the height of the COVID response, FEMA encountered and responded to disinformation claiming that FEMA was removing Personal Protective Equipment from various communities. Similarly, following Hurricane Sandy’s landfall in 2012, FEMA responded to falsehoods related to the safety of drinking water, bridge failures, and locations of shelters to share accurate information with the public.

*Building resilience to disinformation narratives by raising awareness of the threat and of techniques to reenforce digital literacy.*

Several DHS components seek to increase public understanding of what disinformation is and how they can recognize it. For example, CISA has produced a series of graphic novels and publications to raise public awareness about disinformation and foreign influence operations.<sup>8</sup> CISA circulates educational information that explains how disinformation exploits the user and how to identify signs of disinformation. DHS’s Center for Prevention Programs and Partnerships (CP3) provides online resources and the DHS’s Targeted Violence and Terrorism Prevention Grant Program funds projects that promote digital literacy. Likewise, FEMA conducts training

---

<sup>8</sup> See, e.g., *The War on Pineapple: Understanding Foreign Interference in 5 Steps*, CISA (July 2019), [https://www.cisa.gov/sites/default/files/publications/19\\_1008\\_cisa\\_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf](https://www.cisa.gov/sites/default/files/publications/19_1008_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf).

on digital literacy, and DHS’s Science and Technology Directorate conducts and funds research on disinformation trends as well as on ways to mitigate the impact of disinformation through digital literacy.

**c. Analogues Across Government**

**While the components of the Department of Homeland Security have some of the most compelling reasons to address disinformation that could undermine their missions, other agencies of government have for decades taken similar steps without controversy.** For example, the National Oceanic and Atmospheric Administration (NOAA) has responsibility for the dissemination of accurate information about climate, weather, oceans, and coasts for use by the nation’s communities, businesses, and individuals in their daily lives. If disinformation about these issues undermines that mission, it will take steps to disseminate correct information. The Department of Transportation’s National Highway Traffic and Safety Administration (NHTSA) similarly has the authority to provide accurate information to the public by notifying vehicle owners of defects and how to remedy them. The Department of Health and Human Services publishes Health Misinformation Advisories. As the U.S. Surgeon General has said, “Health misinformation is a serious threat to public health. It can cause confusion, sow mistrust, harm people’s health, and undermine public health efforts.”<sup>9</sup> These are but three examples of the ways in which other governmental entities routinely further agency missions by providing accurate information to the public and responding to disinformation.

## RECOMMENDATIONS

---

Here are our recommendations:

**(1) It is Imperative that DHS Address Inaccurate Information that Undermines its Critical Missions**

We previously recommended to the full Council—and the Council has accepted our recommendation—that there is no need for a separate Disinformation Governance Board. But it is our assessment that the underlying work of Department components on this issue is critical. **The Department must be able to address the disinformation threat streams that can undermine the security of our homeland.**

The Department cannot render effective service to the American people without being able to speak authoritatively and accurately to the public. **Critically, this work can and must be undertaken consistent with the law and best practices.**

**To address its Congressionally mandated missions, the Department needs the ability to**

---

<sup>9</sup> Vivek H. Murthy, *Foreword* to CONFRONTING HEALTH MISINFORMATION: THE U.S. SURGEON GENERAL’S ADVISORY ON BUILDING A HEALTHY INFORMATION ENVIRONMENT (2021), <https://www.ncbi.nlm.nih.gov/books/NBK572171/>.

**identify, analyze, and, where necessary, address certain incorrect information, especially but not limited to information that tends to undermine public safety and malicious efforts by foreign governments and foreign actors to manipulate the American public.**

We emphasize, in this regard, that **the Department of Homeland Security does not have a broad remit to address all inaccurate information or disinformation, nor does it have the authority to silence or sanction anyone's speech. Rather, its efforts should focus on (a) assessing whether publicly disseminated disinformation impedes missions assigned to the agency by law and (b) disseminating correct information.**

**The Department can and should speak publicly to accurately inform the public of disinformation.** The Department already engages in much of this activity to good effect. These public communications efforts can include publishing a factual correction, publishing additional context, identifying the source of the disinformation as a foreign actor, informing the public about issues relating to the credibility of the disseminator—such as by revealing facts that show a motive to lie or a conflict of interest—disclosing that the author is using a false identity, or revealing past falsehoods, for example. Apart from these public rebuttals, **the Department can and should also bring such disinformation to the attention of other government agencies for appropriate action and to platforms hosting the falsehoods.** It is for the platforms, alone, to determine whether any action is appropriate under their policies.

Given the centrality of this recommendation, we highlight here what these activities mean in practice. Assume that a false statement that FEMA is setting forest fires goes viral on the Internet, leading to threats of violence against FEMA personnel. FEMA should address that rumor. This is the sort of routine step that government agencies take to correct the record, as necessary, to provide accurate information to the public about what the agency is or is not doing. Likewise, a FEMA official recently warned that vulnerabilities in software used in television and radio networks across the country to transmit emergency alerts could be hacked by a malicious actor to broadcast false messages. Were hackers to use emergency systems to transmit such erroneous alerts and sow chaos and confusion, FEMA would have to respond.

In another hypothetical example, widely believed false statements that one should never install software patches or updates on computers, or that one can always be confident that links in emails are safe to click, would impede CISA's mission to protect our cybersecurity. CISA would need to speak publicly to explain to the public the truth about patching software and practicing proper cybersecurity hygiene.

Similarly, false information about the time, place and manner of voting—for example, an official-looking statement that tells people of one party that in-person voting is on a day that is not the actual date of an election—undermines CISA's mission of protecting the critical infrastructure of our electoral process. CISA needs to address such disinformation. It can and must do so consistent with the law.

**There is a particularly heightened need to address foreign-influence operations by nation-states or other foreign adversaries.** China, Iran, Russia, and others have engaged in aggressive information operations targeting U.S. interests and U.S. domestic stability. For example, a

bipartisan investigation by the U.S. Senate Select Committee on Intelligence found that Russian authorities interfered in the 2016 presidential election in a far-ranging influence campaign “to spread disinformation, divide the public, and undermine our democracy,” in the words of Committee Chairman Sen. Richard Burr (R-NC).<sup>10</sup> Similarly, during the 2020 election, Iranian adversaries posed as members of the Proud Boys group, urging actions that would undermine our elections.<sup>11</sup> These foreign actors use both state media and, more perniciously, proxy websites and social media platforms to create and amplify narratives that further their ends. The Department has a responsibility to protect our national security by warning of these activities and sharing this information with other relevant government agencies.

As noted, I&A conveys information to other DHS components, and to federal, state, and local partners, about emerging trends in foreign adversary disinformation and other influence operations. As discussed below, we believe I&A should bolster its efforts in this regard.

## **(2) DHS Must Assure that Standards are Maintained**

**The components of the Department responsible for the protection of legal and civil rights and liberties should enhance their interaction with the components that have operational roles in this area, to provide assurance that the work of Departmental components is consistent with the law and the relevant civil rights and privacy protections.**

The Department’s Office of General Counsel, the Department’s Privacy Office, and the Department’s Office for Civil Rights and Civil Liberties (CRCL) support the Department’s mission to secure the nation while preserving individual liberty, fairness, and equality under the law, to include setting policies for each component, especially with respect to the requirements and constraints mandated by legal, privacy, and civil rights and civil liberties responsibilities. These policies are properly assembled by the relevant legal, privacy, and civil rights officers and conveyed to the relevant components and among Department senior leadership. **We recommend that these offices be tasked with affirmative engagement with each of the relevant components on a regular basis to ensure that operational components are implementing that guidance; that they routinely review the work of the components to ensure compliance with such guidance; and that they review and, as needed, update rules governing the analysis of disinformation and permissible responses.**

Additionally, because all DHS components confront erroneous or misleading information that poses a threat to their mission, **the Office of Public Affairs should be tasked with engaging on a regular basis with the public affairs offices in each of the components so that public statements about disinformation are made in a consistent manner and benefit from best practices across the Department.**

---

<sup>10</sup> *Senate Intel Committee Releases Bipartisan Report on Russia’s Use of Social Media*, U.S. Senate Select Committee on Intelligence (Oct. 8, 2019), <https://www.intelligence.senate.gov/press/senate-intel-committee-releases-bipartisan-report-russia%E2%80%99s-use-social-media>. The Senate report affirmed similar conclusions by the U.S. Intelligence Community and the investigation of the U.S. Department of Justice Special Counsel.

<sup>11</sup> *Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election*, U.S. Dep’t of Justice (Nov. 18, 2021), <https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed>.

**(3) DHS Should Assure that the Department Has the Technical Expertise to Confront Future Threats**

Those who utilize disinformation to threaten our domestic security are constantly enhancing their techniques and their strategies. The capabilities of the Department's components are uneven. **We recommend that I&A, with support from the Directorate of Science and Technology, ensure that the Department and its components have the technical capability to address future challenges related to disinformation. In particular, this should include analysis of strategic trends in disinformation content, identification of significant disinformation propagators, and explanation of technologies being used to amplify, mask, or intensify disinformation, including through the propagation of synthetic media or "deepfakes."**

**(4) DHS Should Bolster the Role of the Office of Intelligence and Analysis**

I&A should serve as a principal channel for obtaining disinformation warnings from the U.S. Intelligence Community and from other entities. I&A should furnish to other components guidance and notice of significant disinformation threats to DHS missions, such as:

- Foreign influence operations;
- Domestic Violent Extremist-driven disinformation that elevates risks of violence;
- The identity of high-volume disinformation purveyors;
- Emerging focal points of disinformation, such as dangerously inaccurate health advice; and
- Emerging technologies that intensify dissemination and the targeting of disinformation.

**(5) DHS Should Promote Transparency**

Secretary Mayorkas directed the subcommittee to provide recommendations for how to achieve greater transparency across the Department's disinformation-related work, including to increase trust among the public and other key stakeholders, in a way that could serve as a model for achieving transparency in other mission areas.

**Disinformation spreads when authoritative voices are absent or untrustworthy. To counter these challenges, we recommend the Department adopt the following recommendations, which may be useful across DHS missions:**

**1. Communicate Consistently.** In our review, we have been impressed by the important, necessary work that DHS components do to respond to inaccurate information that threatens the security of the country. The Department and its components should explain how its actions protect the homeland, further DHS's missions, and safeguard Americans.

**2. Speak Clearly.** There is very little public awareness of what the Department actually does in addressing disinformation. This field is saturated with terms that many Americans find impenetrable and even threatening when, in fact, what the Department and its components do is provide to the public or otherwise

disseminate accurate information in the face of dangerous disinformation. When discussing these issues with the public, the Department should use plain language, describe actual examples, and explain the benefits of its activities, and the limitations on DHS's activities.

**3. Emphasize Principles.** In addition to explaining what it does and how, the Department should also make clear the legal and constitutional boundaries that guide its work. It should more actively explain that it does not—and, legally, cannot—interfere with citizens' First Amendment rights and that partisan political considerations play no role in efforts to respond to inaccurate speech. The Department should take every opportunity to assure the public of the clear guardrails that guide its work.



## **APPENDIX 1: EXAMPLES OF DISINFORMATION IMPAIRING DHS'S CORE MISSIONS AND EXAMPLES OF PRODUCTS RELEASED**

---

### **A. Examples of Disinformation Impacting DHS's Core Missions**

#### *Cybersecurity and Infrastructure Security Agency (CISA)*

- **Election Security:** Disinformation undermines confidence in the security of U.S. elections. False statements on this topic have had significant operational impacts on U.S. elections and election offices through increased threats to election workers, which has led to increased attrition of election workers.
- **Critical Infrastructure:** The spread of disinformation has led to material threats to critical infrastructure targeting public health, communications, financial services, the defense industrial base, and rare-earth mineral producers, which are critical to U.S. security. These threats impact the operations of critical infrastructure, their finances, and reputations. For example, in the early summer of 2020, a conspiracy spread widely online that 5G cell towers are responsible for the spread of the coronavirus, leading to attacks on cell phone towers and telecommunications workers, particularly in the United Kingdom, continental Europe, and New Zealand. As a result, DHS issued an advisory to the U.S. telecommunications industry that the dangers of coronavirus conspiracists inciting attacks against communications infrastructure would probably increase as the disease spread.

#### *U.S. Customs and Border Protection (CBP)*

- To lure migrants to the border, smugglers (or “coyotes”) have spread false statements that anyone smuggled into the United States receives asylum and that pregnant women will be allowed into the country.
- CBP has seen many examples of smugglers’ ads on social media and in chat rooms in Spanish and English claiming they can get migrants safely into the United States for a price. Ads also offer counterfeit identification documents and target specific nationalities or groups. This disinformation drives migration to the United States, endangers the lives of migrants, and undermines the Department’s mission to secure the nation’s borders.

#### *The Federal Emergency Management Agency (FEMA)*

- FEMA has seen how disinformation has targeted victims of natural disasters.
- For example, FEMA has observed a rise in disinformation targeting individuals via text or direct messaging, telling them to send their bank account information to a particular address or website in order to receive FEMA assistance. These scams allow bad actors to compromise the victims’ bank accounts.

- The agency has also tracked the spread of false rumors that FEMA is giving out gift cards or that FEMA is picking up debris from private property. These myths negatively impact FEMA's mission.
- False narratives can also lead to offline actions that threaten the safety and security of responder personnel and/or disaster survivors, cause operational disruptions that impede disaster response and recovery efforts, and diminish public trust and confidence in the agency.

*United States Secret Service (Secret Service)*

- The Secret Service is aware that disinformation has the potential to impact its protective mission. For example, malicious entities could post disinformation on social media platforms that could resonate with radical or malicious groups, causing them to disrupt the security plan of a protected site or threaten a protectee.

**B. Examples of Products Released and Activities Undertaken by DHS Components to Address Disinformation**

*Cybersecurity and Infrastructure Security Agency<sup>12</sup>*

- **CISA Insights: COVID-19 Disinformation Activity:** CISA Insights publication that provides an overview of coronavirus disinformation and steps that can be taken to reduce the risk of sharing inaccurate information with your friends and family.<sup>13</sup>
- **CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure:** CISA Insights publication that provides critical infrastructure owners and operators with guidance on how identify and mitigate the risks of influence operations using mis-, dis-, and malinformation (MDM) narratives from steering public opinion and impacting critical infrastructure and National Critical Functions, which are functions of government and the private sector so vital to the United States that their disruption would have a debilitating effect on national security or safety.<sup>14</sup>
- **COVID-19 Disinformation Toolkit:** A toolkit publication downloadable from CISA's website that includes talking points, FAQs, outreach graphics, and a poster. It was designed to help state, local, tribal, and territorial officials bring awareness to misinformation, disinformation, and conspiracy theories appearing online related to COVID-19's origin, scale, government response, prevention and treatment. Each product can be designed to be tailored with local government websites and logos.<sup>15</sup>

---

<sup>12</sup> <https://www.cisa.gov/mdm>, <https://www.cisa.gov/mdm-resource-library>.

<sup>13</sup> [https://www.cisa.gov/sites/default/files/publications/CISAInsights-COVID-19\\_Disinformation\\_Activity\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/CISAInsights-COVID-19_Disinformation_Activity_508.pdf).

<sup>14</sup> [https://www.cisa.gov/sites/default/files/publications/cisa\\_insight\\_mitigating\\_foreign\\_influence\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/cisa_insight_mitigating_foreign_influence_508.pdf).

<sup>15</sup> <https://www.cisa.gov/covid-19-disinformation-toolkit>.

- **Disinformation Stops With You Infographic Set:** A set of infographics (in English and Spanish) that provides an overview of mis-, dis-, and malinformation and five proactive steps that individuals can take to help stop the spread of disinformation: recognize the risk, question the source, investigate the issue, think before you link, and talk to your circle.<sup>16</sup>
- **Foreign Interference Taxonomy:** An infographic overview of terms used to describe different kinds of foreign influence activities for the purpose of undermining the interests of the United States and its allies, provided in both English and Spanish.<sup>17</sup>
- **Graphic Novel - Bug Bytes:** Part of the Resilience series,<sup>18</sup> Bug Bytes demonstrates how threat actors use social media and other communication platforms to spread inaccurate information for the sole purpose of planting doubt in the minds of targeted audiences to steer their opinion. Readers follow protagonist Ava, a graduate, who uses her wits and journalism skills to uncover a disinformation campaign set to damage Fifth Generation (5G) critical communications infrastructure in the United States.<sup>19</sup>
- **Graphic Novel - Real Fake:** Part of the Resilience series, Real Fake demonstrates how threat actors capitalize on political and social issues (especially around election cycles) to stealthily plant doubt in the minds of targeted audiences and steer their opinion. Readers follow protagonists Rachel and Andre as they discover that a command center in Russia is using a network of troll farms to spread false narratives about elections to American voters. With the elections coming up, Rachel and Andre follow the trail of synthetic media and stop the cyber assailants from causing chaos, confusion, and division.<sup>20</sup>
- **Information Manipulation Infographic:** This English- and Spanish-language infographic highlights tactics used by disinformation campaigns (e.g., manipulating content service providers or defacing public websites) that seek to disrupt American life and the infrastructure that underlies it. It includes use of new and traditional media to amplify divides and foment unrest in the homeland, sometimes coordinated with illicit cyber activities.<sup>21</sup>
- **Mis-, Dis-, and Malinformation Planning and Incident Response Guide for Election Officials:** Developed by the Election Infrastructure Subsector's Government Coordinating Council (GCC) and Subsector Coordinating Council's (SCC) Mis/Disinformation Working Group, this guide explains how to recognize, prepare for, and respond to MDM threats that may impact the ability to conduct elections.<sup>22</sup>

<sup>16</sup> [https://www.cisa.gov/sites/default/files/publications/disinformation\\_stops\\_with\\_you\\_infographic\\_set\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/disinformation_stops_with_you_infographic_set_508.pdf), [https://www.cisa.gov/sites/default/files/publications/disinformation\\_stops\\_with\\_you\\_infographics\\_spanish\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/disinformation_stops_with_you_infographics_spanish_508.pdf).

<sup>17</sup> [https://www.cisa.gov/sites/default/files/publications/foreign\\_interference\\_taxonomy\\_october\\_15.pdf](https://www.cisa.gov/sites/default/files/publications/foreign_interference_taxonomy_october_15.pdf), [https://www.cisa.gov/sites/default/files/publications/foreign\\_interference\\_taxonomy\\_spanish\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/foreign_interference_taxonomy_spanish_508.pdf).

<sup>18</sup> <https://www.cisa.gov/resilience-series-graphic-novels>.

<sup>19</sup> [https://www.cisa.gov/sites/default/files/publications/bug\\_bytes\\_graphic\\_novel\\_508\\_v2.pdf](https://www.cisa.gov/sites/default/files/publications/bug_bytes_graphic_novel_508_v2.pdf).

<sup>20</sup> [https://www.cisa.gov/sites/default/files/publications/cfi\\_real-fake\\_graphic-novel\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/cfi_real-fake_graphic-novel_508.pdf).

<sup>21</sup> [https://www.cisa.gov/sites/default/files/publications/information\\_manipulation\\_infographic\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/information_manipulation_infographic_508.pdf), [https://www.cisa.gov/sites/default/files/publications/information\\_manipulation\\_spanish\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/information_manipulation_spanish_508.pdf).

<sup>22</sup> [https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/mdm-incident-response-guide_508.pdf).

- **Rumor Control Page Start-Up Guide:** Developed by the Election Infrastructure Subsector's Government Coordinating Council (GCC) and Subsector Coordinating Council's (SCC) Mis/Disinformation Working Group, this is a guide for election officials on how and when to develop a rumor control webpage to dispel specific MDM narratives through transparent and authoritative information.<sup>23</sup>
- **Social Media Bots Infographic Set:** These infographics are designed to help Americans understand how bots, which are automated programs, simulate human behavior on social media platforms, and how bad actors use social media bots to spread false or misleading information, shut down opposition, and elevate their own platforms for further manipulation. They are available in English and Spanish.<sup>24</sup>
- **Tools of Disinformation: Inauthentic Content:** This flyer (available in English and Spanish) highlights the tactics used by disinformation campaigns such as manipulating audio and videos, conducting forgeries, and developing proxy websites in order to undermine public confidence and sow confusion.<sup>25</sup>
- **War on Pineapple: Understanding Foreign Interference in 5 Steps:** This infographic, with a tongue-in-cheek approach to putting pineapple on pizza, looks at how foreign adversaries conduct malign information operations to inflame hot button issues in the United States. It is available in English and Spanish.<sup>26</sup>

*Office of Intelligence and Analysis (I&A)*

I&A writes products on disinformation and countering foreign influence that are disseminated within the government. I&A also runs mission centers that serve as the Department's center of gravity for intelligence-driven integration of analysis, technology, skills, and functions to counter the most critical threats facing the homeland.

Each Mission Center is tasked with a topical mission goal focused on mitigating enduring threats to the homeland. Mission Centers collect information to address DHS and national intelligence priorities and provide available reporting gathered by DHS components and state, local, tribal, and territorial partners to the Intelligence Community and other customers. Many of our Mission Centers utilize the Homeland Security Information Network to share sensitive, but unclassified information. This network is used to manage operations, analyze data, send alerts and share the information that is necessary to ensure the homeland is safe, secure, and resilient.

Among I&A's mission centers is the Cyber Mission Center (CYMC), the Department's premier provider for cyber threat analysis. CYMC delivers finished intelligence to enable the

<sup>23</sup> [https://www.cisa.gov/sites/default/files/publications/rumor-control-startup-guide\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/rumor-control-startup-guide_508.pdf).

<sup>24</sup> [https://www.cisa.gov/sites/default/files/publications/social\\_media\\_bots\\_infographic\\_set\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/social_media_bots_infographic_set_508.pdf),  
[https://www.cisa.gov/sites/default/files/publications/social-media-bots-infographic-set-spanish\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/social-media-bots-infographic-set-spanish_508.pdf).

<sup>25</sup> [https://www.cisa.gov/sites/default/files/publications/mdm-inauthentic-content-product-english\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/mdm-inauthentic-content-product-english_508.pdf),  
[https://www.cisa.gov/sites/default/files/publications/mdm-inauthentic-content-product-spanish\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/mdm-inauthentic-content-product-spanish_508.pdf).

<sup>26</sup> [https://www.cisa.gov/sites/default/files/publications/19\\_1008\\_cisa\\_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf](https://www.cisa.gov/sites/default/files/publications/19_1008_cisa_the-war-on-pineapple-understanding-foreign-interference-in-5-steps.pdf), [https://www.cisa.gov/sites/default/files/publications/war-on-pineapple-spanish\\_508.pdf](https://www.cisa.gov/sites/default/files/publications/war-on-pineapple-spanish_508.pdf).

Department's mission of ensuring cybersecurity and resilience of the federal government, our State, Local, Tribal, and Territorial partners and critical infrastructure networks. It works to expand this capability while also evolving the DHS Intelligence Enterprise cyber program through closer integration across intelligence networks.<sup>27</sup>

### *U.S. Customs and Border Protection*

The CBP Office of Public Affairs leads the agency in their efforts to combat disinformation. Many of those efforts are targeted at border crossing disinformation put out by criminals and others standing to profit from vulnerable populations. CBP hosted reporters from six countries recently for a border visit to show them the realities of irregular migration, the dangers associated, and to push back on the lies smugglers use.

- **Digital Ad Campaign “Say No to the Coyote”:** CBP launched a digital advertisement campaign to dissuade migrants in the Northern Triangle countries of Honduras and Guatemala who might consider taking the dangerous journey to the U.S. border. The ads deliver a clear message: smugglers (or, coyotes) are lying to you, the fact is that entering the United States illegally is a crime. The ads highlight that smugglers take advantage of and profit from vulnerable migrants.
  - For years, CBP has run ad campaigns to dissuade migrants from putting their lives in the hands of smugglers and to inform them of the U.S. immigration laws in place. These ads are an expansion of those efforts.
  - The message warns that those attempting to cross the U.S. border without authorization will be immediately removed from the country or placed into immigration removal proceedings. Users are also reminded of the thousands who are jailed, kidnapped, extorted, or even left to die by unscrupulous transnational criminal organizations. The ad includes additional creative displays that users are invited to share through messaging apps or through social media.<sup>28</sup>

### *The Federal Emergency Management Agency*

Rumor control is a common practice for emergency communication practitioners and is routinely included in disaster drills and exercises in addition to being used in real-world events. Rumors can be identified by the public, agency stakeholders such as congressional or elected officials, private sector or voluntary organizations, or by the media. Social media has accelerated the spread of rumors but also enhanced the speed at which an agency or organization may share rumor corrections directly with the public.

- **Hurricane Sandy:** During the Hurricane Sandy response in 2012, FEMA responded to rumors related to the safety of drinking water, bridge failures, and locations of shelters to share accurate information with the public. These rumors were often fueled by social media

<sup>27</sup> <https://www.dhs.gov/mission-centers>.

<sup>28</sup> <https://www.cbp.gov/coyote-criminal>, <https://www.cbp.gov/newsroom/national-media-release/cbp-launches-digital-ad-campaign-say-no-coyote-warn-migrants-about>.

posts and FEMA has since built capacity to identify and respond to rumors during all disaster responses.

- **Rumor Control Webpages:** During major disaster responses like Hurricane Maria, the COVID-19 pandemic, and more recently Hurricane Ida, FEMA has established Rumor Control webpages and leveraged its social media accounts to share accurate information and address misconceptions. FEMA also frequently anticipates common rumor and misinformation topics after a disaster, such as those regarding specific types of disaster assistance available and scams that target disaster survivors.<sup>29</sup>
- **Office of External Affairs:** FEMA identifies rumors by leveraging a team in its Office of External Affairs to conduct searches on social media for public conversations. That team analyzes the information to support situational awareness during disaster responses. In some cases, FEMA also receives reports from federal partners, like CISA and the Department of State.
- **Hurricane Florence:** After Hurricane Florence made landfall, a large amount of incorrect information was circulating on social media related to FEMA and the state's role in the response. To ensure an effective response, FEMA's Office of External Affairs, in coordination with various teams, took steps to provide accurate, authoritative information to the public. It created a webpage on FEMA's website. As new false information circulated online, the agency posted correct information to the website to provide clear, authoritative information to address each rumor. Agencies shared these rumor-control messages themselves and with state and local partners.

---

<sup>29</sup> <https://www.fema.gov/disaster/coronavirus/rumor-control>.

## **APPENDIX 2: COMPILATION OF PRODUCTS**

---

Appendix 2 is a compilation of many of the products listed in subsection (B). It may be found in the enclosed attachment, titled “*HSAC Disinformation Subcommittee Final Report Appendix 2.*”

**APPENDIX 3: TASKING LETTER**

Secretary

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

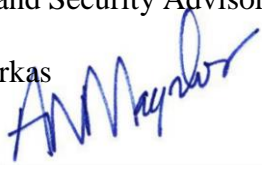


**Homeland  
Security**

May 18, 2022

MEMORANDUM FOR: William J. Bratton  
Jamie Gorelick  
Co-Chairs, Homeland Security Advisory Council

CC: Karen Tandy  
Vice Chair, Homeland Security Advisory Council

FROM: Alejandro N. Mayorkas  
Secretary 

SUBJECT: **Initial Homeland Security Advisory Council Projects**

Thank you again for agreeing to serve as Co-Chairs of the Homeland Security Advisory Council (HSAC). I benefited greatly from our March 21, 2022 meeting and appreciated the insights and contributions of all the HSAC Members in attendance.

In our meeting, we identified a series of projects that the HSAC could undertake in a wide range of areas of importance to the Department. I am writing to request that the HSAC initially undertake two projects, with the understanding that others are forthcoming.

For the first project, I request that a group of HSAC members assess how the Department can most effectively and appropriately address disinformation that poses a threat to the homeland, while increasing transparency and protecting free speech, civil rights, civil liberties, and privacy. For almost a decade, the Department has worked to address this particular form of disinformation and I want to ensure we do everything possible to instill trust that we are protecting core Constitutional rights across our work.

I request that the HSAC submit its findings and key recommendations to me within 75 days of the date of this memorandum, consistent with applicable rules and regulations. DHS will transmit the final report to Congress and make it available to the public.

The second is a project we identified in our meeting in March. I request that a group of HSAC members assess how the Department can improve our customer experience and service delivery mechanisms to meet customer and community needs, including by leveraging technology and other innovations and increasing efficiency.

I request that the HSAC submit its findings and key recommendations to me within 120 days of the date of this memorandum, consistent with applicable rules and regulations. DHS will also transmit this final report to Congress and make it available to the public.



These two initial projects will call on the expertise of HSAC Members and will be of tremendous value to the Department. Thank you for your service on the HSAC and to our nation.

### **Assessment of Disinformation Best Practices and Safeguards**

For nearly ten years, across multiple Administrations, the Department has sought to understand and address the threat posed specifically by disinformation that endangers our homeland security. This includes disinformation spread by foreign states such as Russia, China, and Iran, foreign adversaries such as transnational criminal organizations and human smuggling organizations, and criminals seeking to victimize vulnerable members of the American public in times of significant distress. The Department is committed to ensuring this work does not infringe on freedom of speech, civil rights, civil liberties, and privacy.

I request that Jamie Gorelick and Michael Chertoff be designated to lead this assessment, which will include, but need not be limited to, the following:

1. Recommendations for how the Department can most effectively and appropriately address disinformation that poses a threat to the homeland, while protecting free speech, civil rights, civil liberties, and privacy, including through proposed unified principles to guide the Department's disinformation-related work; and,
2. Recommendations for how to achieve greater transparency across our disinformation-related work, including to increase trust with the public and other key stakeholders, in a way that could serve as a model for achieving transparency in other mission areas.

### **Assessment of Customer Experience and Service Delivery**

DHS interacts with the public on a daily basis more than any other federal agency. It is among our top priorities to ensure we are effectively meeting the needs of the diverse communities we serve. To this end, we are focused on facilitating lawful trade and travel more efficiently, modernizing our ports of entry and border processing, increasing equity in disaster assistance programs, streamlining the process to deliver legal immigration benefits, increasing our transparency and openness with the public, strengthening the cybersecurity of public and private sector partners, and much more.

The assessment of our customer experience and service delivery mechanisms will include, but need not be limited to, the following:

1. Recommendations for how to better design the Department's delivery of services to meet customer and community needs, including by (a) leveraging technology and other innovations to reduce burdens on the public, and (b) increasing the adoption of best practices to maximize efficiency and improve the customer experience across relevant mission areas;
2. Recommendations for how the Department can measure customer experience and service delivery effectiveness, establish targets for improvement, and ensure that our programs, policies, and operations improve equity and protect privacy, civil rights, and civil liberties; and,
3. Recommendations for how the Department can better exchange with the private sector the knowledge, talent, and best practices around customer experience and service delivery, such as through executives-in-residence and public sector leave programs.

I look forward to discussing the assessments with you and other Members of the HSAC. Thank you again for your service as Co-Chairs.

## APPENDIX 4: SUBCOMMITTEE MEMBER BIOGRAPHIES



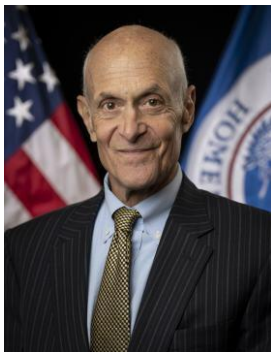
**Jamie Gorelick (Co-Chair)**

Partner

Wilmer Cutler Pickering Hale and Dorr, LLP

Ms. Jamie Gorelick (HSAC Co-Chair) is presently a Partner at the WilmerHale law firm where she represents institutions and individuals in a wide array of matters, particularly in the regulatory and enforcement arenas, addressing issues as diverse as antitrust, environmental regulation, securities enforcement, and national security.

Ms. Gorelick was one of the longest serving Deputy Attorneys General of the U.S. In that role, she supervised the entire Department of Justice, including its litigation and law enforcement divisions and the U.S. Attorneys' Offices. Ms. Gorelick also served as General Counsel of the Department of Defense, where she helped structure the Department's involvement in the consolidation of the defense industry. She was awarded the Secretary of Defense Distinguished Service Medal. Earlier in her career, Ms. Gorelick was Vice Chair of the Task Force on the Audit, Inspection, and Investigation Components of the Department of Defense. She was also Counselor to the Deputy Secretary of Energy and Assistant to the Secretary. Ms. Gorelick was a member of the bipartisan National Commission on Terrorist Attacks Upon the United States (the "9/11 Commission") and she has served on many government boards and commissions.



**Michael Chertoff (Co-Chair)**

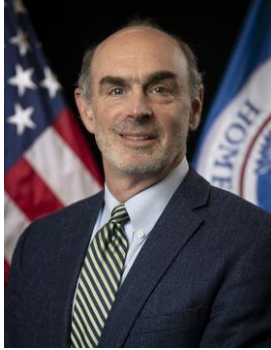
Former Secretary of DHS and Co-Founder

The Chertoff Group

As Secretary of the U.S. Department of Homeland Security from 2005 to 2009, Mr. Michael Chertoff led the country in blocking would-be terrorists from crossing our borders or implementing their plans if they were already in the country. He also transformed FEMA into an effective organization following Hurricane Katrina. At Chertoff Group, Mr. Chertoff provides high-level strategic counsel to corporate and government leaders on a

broad range of security issues, from risk identification and prevention to preparedness, response and recovery.

Before heading up the Department of Homeland Security, Mr. Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit. Earlier, during more than a decade as a federal prosecutor, he investigated and prosecuted cases of political corruption, organized crime, corporate fraud, and terrorism – including the investigation of the 9/11 terrorist attacks. In addition to his role at Chertoff Group, Mr. Chertoff is also senior counsel at Covington & Burling LLP.



**Ted Schlein**  
General Partner  
Kleiner Perkins  
Executive Chairman  
Ballistic Ventures

Mr. Ted Schlein is a general partner at Kleiner Perkins, and executive chairman and founding partner at Ballistic Ventures. Mr. Schlein has spent the last 35 years helping to create transformative companies.

A Midas of investing and the former chairman of the National Venture Capital Association (NVCA), Mr. Schlein has served on over 50 public and private company boards, which include many of the world's greatest cybersecurity companies. As a company leader, he was the founding CEO of Fortify Software, which was later acquired by Hewlett-Packard.

Prior to Kleiner and Ballistic, Mr. Schlein served as vice president, Enterprise Solutions at Symantec. There he led the company's earliest antivirus effort, which included a move into the software utilities market with the launch of a commercial antivirus solution that became the industry gold standard. Mr. Schlein is an active member of the CISA Cybersecurity Advisory Committee, National Security Institute Advisory Board, and the Council on Foreign Relations, Independent Task Force on Cybersecurity.



**Ms. Sonal Shah**  
Executive Vice President, Worldwide Network Operations  
United Way Worldwide  
Founding President  
The Asian American Foundation

Ms. Sonal Shah is currently the Executive Vice President at United Way Worldwide managing the domestic and international operations. She was the Founding President of The Asian American Foundation, launching the largest non-philanthropic effort for the Asian American community. Prior

to this role, Ms. Shah founded and led the Beeck Center for Social Impact & Innovation at Georgetown University. Ms. Shah, one of the foremost global leaders on social impact and innovation, has worked in government, business, and the nonprofit sectors.

During the Obama Administration, Ms. Shah served as the Deputy Assistant to the President and founding Director of the White House Office of Social Innovation and Civic Participation. More recently, Ms. Shah served as the National Policy Director for Mr. Pete Buttigieg's run in the 2020 presidential election.

Ms. Shah spent seven years at the U.S. Department of Treasury where she was an international economist working on post conflict reconstruction and international finance. She has led efforts at Goldman Sachs developing their environmental strategy and implementation. She also led Google's global development initiatives focusing on finance and technology for development. She also has tremendous experience developing policy working at the Center for American Progress and the Center for Global Development focusing on trade and economic development. Ms. Shah is a co-founder of Indicorps, a nonprofit with the goal of building a new generation of socially conscious global leaders.



**Ali Soufan**  
Chairman and CEO  
The Soufan Group, LLC

Mr. Ali H. Soufan is the Chairman and CEO of The Soufan Group, LLC, and has been a member of the Homeland Security Advisory Council since September 2012.

Mr. Soufan is a former FBI Supervisory Special Agent who investigated and supervised highly sensitive and complex international terrorism cases, including the East Africa Embassy Bombings, the attack on the USS Cole, and the events surrounding the 9/11 attacks. In addition, he served on the Joint Terrorist Task Force, FBI New York Office, where he coordinated both domestic and international counterterrorism operations.



**Matthew F. Ferraro**  
Counsel  
Wilmer Cutler Pickering Hale and Dorr, LLP

Matthew F. Ferraro is counsel in the Washington, DC office of Wilmer Cutler Pickering Hale and Dorr LLP where he practices at the intersection of national security, cybersecurity, and crisis management. He counsels clients, writes, and speaks on the threats that viral disinformation and deepfakes pose to corporations, brands and markets, on the positive-use applications of synthetic media, and on this evolving regulatory environment, which he calls “disinformation and deepfakes risk management” (DDRM). In the mergers and acquisitions sector, Mr. Ferraro helps clients navigate complex transactions before the Committee on Foreign Investment in the United States (CFIUS). In the cyber domain, Mr. Ferraro regularly works with companies to prepare for and respond to cyberattacks, including ransomware incidents.

Earlier in his career, Mr. Ferraro was a U.S. intelligence officer and held staff, policy, and operational positions at the Office of the Director of National Intelligence and the Central Intelligence Agency. He is a term member of the Council on Foreign Relations and a senior fellow at the National Security Institute at George Mason University. Born and raised in New York City, Mr. Ferraro was educated at Yale, Cambridge, and Stanford universities.

## APPENDIX 5: SUBJECT MATTER EXPERTS AND OTHER WITNESSES

Robert Silvers	Under Secretary	Office of Strategy, Policy, and Plans
Kenneth Wainstein	Under Secretary	Office of Intelligence and Analysis
Jen Easterly	Director	Cybersecurity and Infrastructure Security Agency (CISA)
Marsha Espinosa	Assistant Secretary	Office of Public Affairs
Samantha Vinograd	(A) Assistant Secretary	Counterterrorism and Threat Prevention
Jennifer Daskal	Deputy General Counsel	Office of General Counsel
Andrew Fausett	Assistant General Counsel	Office of General Counsel
Brian Puchalsky	Attorney Advisor	Office of General Counsel
Scott Mathews	Senior Advisor to the Deputy Chief Privacy Officer	Office of Privacy
Brian Sterling	Section Chief	Office for Civil Rights and Civil Liberties
Nadia Firozvi	Chief of Staff	Office for Civil Rights and Civil Liberties
Kevin Quinn	Senior Policy Advisor	Office for Civil Rights and Civil Liberties
Luis Miranda	Assistant Commissioner	US Customs and Border Protection (CBP), Office of Public Affairs
Geoffrey Hale	National Risk Management Center (NRMC)	Cybersecurity and Infrastructure Security Agency (CISA)
Lucas Hitt	Deputy Director, Office of External Affairs	Federal Emergency Management Agency (FEMA)
Gloria Huang	Digital Engagement and Analytics Branch Chief	Federal Emergency Management Agency (FEMA)
Hannah Vick	Senior Advisor, Office of External Affairs	Federal Emergency Management Agency (FEMA)
Malia Collins	Program Analyst	Federal Emergency Management Agency (FEMA)
Jeffrey Afman	Director, Office of Counterterrorism & Security Preparedness	Federal Emergency Management Agency (FEMA)