



Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Future of DHS Project: Key Findings and Recommendations

Thomas Warrick and Caitlin Durkovich

Research assistance: Mark Massa



Scowcroft Center for Strategy and Security

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

Forward Defense helps the United States and its allies and partners contend with great-power competitors and maintain favorable balances of power. This new practice area in the Scowcroft Center for Strategy and Security produces forward-looking analyses of the trends, technologies, and concepts that will define the future of warfare and the alliances needed for the 21st century. Through the futures we forecast, the scenarios we wargame, and the analyses we produce, *Forward* Defense develops actionable strategies and policies for deterrence and defense, while shaping US and allied operational concepts and the role of defense industry in addressing the most significant military challenges at the heart of great-power competition.

This publication was produced with contributions from SAIC, Accenture Federal Services, CenturyLink, current and former government leaders, and subject-matter experts, under the auspices of a project on refocusing the Department of Homeland Security to protect the American people from the coronavirus, threats to democracy, future threats, and addressing DHS's other major challenges.



Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

Future of DHS Project: Key Findings and Recommendations

Thomas Warrick and Caitlin Durkovich

Research assistance: Mark Massa

ISBN-13: 978-1-61977-116-1

Cover photo: Department of Homeland Security

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The authors are solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

September 2020

Table of Contents

Executive Summary	1
Future of DHS Project: Key Findings and Recommendations	6
I. DHS Needs to Refocus Its Mission to Lead the Defense of the Nation Against Nonmilitary Threats	4
II. DHS's Public-Private Partnerships Are Unique and Should Be Modernized to Effectively Counter the Threats of the 2020s	12
III. Resolving the Issues That Cause DHS's Low Morale	19
IV. Fixing the Internal Challenges That Hold DHS Back	29
Conclusion	34
Annex 1: Glossary of Abbreviations, Acronyms, and Initialisms Used in This Report	35
Endnotes	37
Future of DHS Project: Participant Biographies	42
Acknowledgements	44

Executive Summary

The United States will be less secure, and American democracy will be at risk, unless the Department of Homeland Security (DHS) changes its priorities. Going forward, DHS needs to re-focus its mission to lead the defense of the United States against major nonmilitary threats. DHS needs to modernize its approach to public-private partnerships, fix DHS's most pressing internal problems, and ensure that DHS's actions increase the trust that the American people and DHS's own employees have in what the department does.

DHS's mission is vital to the security and safety of Americans. DHS has more than its share of controversies and challenges, but the solution to DHS's problems is not to dismantle it, but to make major reforms so that DHS can meet newly emerging threats that—paradoxically—DHS is the best cabinet department to address.

The recommendations below are intended to inform the DHS leadership team in January 2021, regardless of the outcome of the US election:

1. Refocus DHS's Mission to Lead the Defense of the Nation Against Nonmilitary Threats

DHS needs to re-focus its mission around today's most serious threats to the nation. These are not what they were even a few years ago.

The most urgent current threat to the United States is COVID-19. DHS was created to prevent another attack as devastating as 9/11, but the reality as of August 2020 is that COVID-19 is killing more people than 9/11 **every four days**. DHS needs to take a stronger leadership role in mobilizing and prioritizing the increased, coordinated distribution of needed testing and medical supplies, and eventually vaccines, and to coordinate and help fund the infrastructure changes required to make US schools, factories, nursing homes, and offices safe. DHS needs to be more pro-active in future pandemics to sound the national alarm and activate emergency playbooks to ensure the federal government is fully mobilized.

DHS needs to lead the nation's defense against the aggressive, ongoing nonmilitary campaigns of Russia, China, and Iran that are targeting American democracy itself. These hostile nation-states, at this moment, are carrying out cyber operations, threatening US election security, attacking American critical infrastructure, creating disinformation, and manipulating social media through covert influence programs. These adversaries' actions seek

to divide Americans and weaken American power, staying just below the level that would justify an American military response. **The United States currently has no effective, integrated, comprehensive defense against this new style of non-kinetic warfare.**

Because DHS has more of the tools to defend against these threats than any other US government department, and because so much of what needs defending is in the hands of state and local governments, the private sector, and individual Americans, **DHS is the department best-suited to lead the defense of the nation against non-kinetic attacks by hostile nation-states.**

The greatest long-term threat to the United States is the effect of climate change or extreme weather on American critical infrastructure. DHS needs to work more closely with state and local governments and the private sector to build greater resilience to hurricanes, floods, fires, and other weather-driven natural disasters to protect more American lives and reduce property damage.

While giving greater attention and resources to the threats listed above, **DHS also needs to maintain its level of resources and efforts on its existing missions.** None of DHS's existing missions are going away. However, **DHS should upgrade its efforts to communicate with the American people, with DHS's stakeholders, and with DHS's own employees. DHS, more than other cabinet departments, needs the trust of the American people and needs to do more to earn that trust.**

For the defense of American democracy to succeed, the secretary of homeland security and DHS generally will need to be, to the greatest extent possible, nonpartisan and "above politics," in the non-partisan traditions of the uniformed military and the US intelligence community.

If DoD's bumper-sticker mission is "We fight and win America's wars," **DHS's mission should be, "We lead the defense of the Nation against non-military threats."**

2. Modernize DHS's Approach to Public-Private Partnerships

Protecting American democracy and building a resilient homeland is a shared endeavor with many stakeholders. This fundamental principle distinguishes DHS's mission from that of other cabinet departments. DHS has the unique ability to convene stakeholders across the homeland security enterprise to solve a crisis or avert a threat.

DHS is not responsible for addressing climate change, but DHS is responsible for working with others, including state and local governments and the private sector, to protect critical infrastructure that is at risk from climate change or extreme weather. Saving lives and infrastructure from hurricanes, floods, fires, and other weather-related events takes continuous and persistent engagement by DHS. Climate change, as noted above, represents the most significant long-term threat to critical infrastructure.

DHS's ability to encourage private-sector companies, some of which compete with each other, to share information to defeat common threats, in cyberspace and elsewhere, is vitally important. This is especially true when nation-states are targeting the US private sector through non-kinetic means. Increasing the speed of information sharing is now vital for both government and industry, as cyberattacks and defenses interact at network speed. The federal government needs to be able to communicate relevant information—including attribution—in real-time to enable increasingly sophisticated companies to prevent damage to their systems or the theft of valuable information. The US Cyberspace Solarium Commission's recommendations to designate "systemically important critical infrastructure" and to have DHS support and lead a Joint Collaborative Environment for the sharing of threat information across the federal government will enhance this effort.

Given the growing threats to our democracy, many of which are targeted at the private sector, DHS should develop a comprehensive engagement strategy to **increase trust and harmonize engagement with key private-sector partners** and make better use of DHS's convening authorities. **DHS also needs to take better advantage of its "retail" presence around the United States, across all its mission areas, and devolve operational support down to the local level.**

3. Address the Workplace Causes of DHS's Low Employee Morale

Given that DHS has been in last place in federal employee morale surveys every year since 2010, DHS should address its workplace and culture issues that are driving employees' low morale. DHS's components at times have experienced some remarkable turnarounds in morale—proof that it can be done at DHS. DHS's focus should be on the Transportation Security Administration

(TSA) and Customs and Border Protection (CBP), which make up half of DHS's workforce. TSA's problems can be improved by addressing low pay, promotions, and career advancement; CBP needs to address problems with trust, how to deal with poor performers, and promotions.

4. Fix DHS's Internal Challenges

DHS needs to make a number of internal reforms. **DHS's decentralized management model needs to change. Policy and budget officials need to work closely together—today, they don't. DHS needs to invest in better communications capability, including greater classified connectivity,** to be able to lead the defense against sophisticated hostile nation-states. **DHS should set up a rotation program,** analogous to DoD's joint duty program, so that **promotion to senior ranks requires a headquarters tour. And DHS should have an "S3" third-ranking official,** just as the Department of Justice does, to coordinate DHS's law enforcement missions.

5. Nominate DHS Senior Leaders Who Can Be Confirmed by the Senate

As of August 1, 2020, more than seventeen of DHS's senior leaders are "acting" or "senior official performing the duties of...." **Not having DHS's senior-most officials confirmed by the Senate undercuts DHS's ability to protect the American people.** A Government Accountability Office (GAO) August 14, 2020, decision said that Acting Secretaries Kevin McAleenan and Chad Wolf and Senior Official Performing the Duties of the Deputy Secretary Ken Cuccinelli were not validly appointed.¹ The DHS's Office of the General Counsel asked the decision to be withdrawn,² but GAO said there was neither a factual nor a legal basis to do so.³ President Trump announced on August 25 his intent to nominate Wolf as secretary of homeland security.

Wolf's confirmation alone will not end the uncertainty at DHS. Private business executives, state and local leaders, labor union leaders, and DHS's own employees all need to know if the senior DHS officials they are dealing with will be around for a while. No one will take a risk or build up a solid relationship of trust with an "acting" official who could be replaced easily or could be gone tomorrow based on a changed legal interpretation. **It is vitally important for the security of the United States that DHS and its components have Senate-confirmed leadership.**

Future of DHS Project: Key Findings and Recommendations

The Atlantic Council's Scowcroft Center for Strategy and Security convened the Future of DHS Project to inform the Department of Homeland Security (DHS) leadership team in January 2021—regardless of the outcome of the 2020 US election—on the direction of DHS's mission and how to address the challenges faced by the department. These key findings and recommendations were written by two former DHS officials, project Director Tom Warrick and Co-Director Caitlin Durkovich, based on input from a Senior Advisory Board of former secretaries and acting secretaries of DHS and a distinguished bipartisan study group of more than 100 homeland and national security experts. The report is the sole responsibility of the authors, and while the report reflects a consensus among the experts, not all study group participants may agree with every recommendation.

The Department of Homeland Security (DHS) needs to refocus its mission to lead the defense of the United States against major nonmilitary threats—infectious diseases; hostile nation-state cyber operations, threats to election security, and foreign disinformation; threats to critical infrastructure from climate change; vulnerabilities in new technologies; and growing white supremacy. DHS was founded in 2003 to focus on the threat from terrorism.⁴ The department was later pushed to take on new missions, but without adequate resources. Today's challenges demand more DHS leadership attention and resources, even as the department still needs to meet all its other current missions. For DHS, nothing goes away.

DHS has more than its share of challenges. Controversies over family separations in 2019 and the deployment of

its officers in cities in the summer of 2020 have raised questions about DHS's core missions—even whether to “abolish DHS.” As of August 1, 2020, seventeen senior DHS officials have “acting” or “performing the duties of” in their titles.⁵ DHS has occupied last place in federal employee morale among large cabinet departments every year since 2010.⁶

The solution to DHS's problems is not to dismantle the department, because what DHS does, or should be doing, is vital to the security and safety of Americans and to national security broadly. DHS is the third largest cabinet department with more than 240,000 employees⁷ and an annual budget of \$62 billion.⁸ Scattering DHS's functions among other cabinet departments would not make those missions and capabilities go away. This report recommends major reforms—driven by strategy and mission priorities—that DHS urgently should undertake so that it can meet the newly emerging threats that—paradoxically—DHS is the best cabinet department to address.

This report sets out in **Part I** the case for a major re-focusing of DHS's mission to address today's greatest non-military threats to the United States. **Part II** makes the case that DHS's ability to harness public-private partnerships today gives it a unique power and obligation among federal departments to help secure and enhance the resilience of the private sector and American communities from traditional and emerging threats, including protecting critical infrastructure from violent extremism, climate change, and a range of threats from hostile nation-states. **Part III** gives specific recommendations to address DHS's single most important management issue: DHS's perennially low employee morale. **Part IV** gives recommendations to address DHS's other most-pressing internal problems that DHS needs to fix to meet today's national security challenges.

Key Findings in blue. Recommendations in black. Topic headings in red.

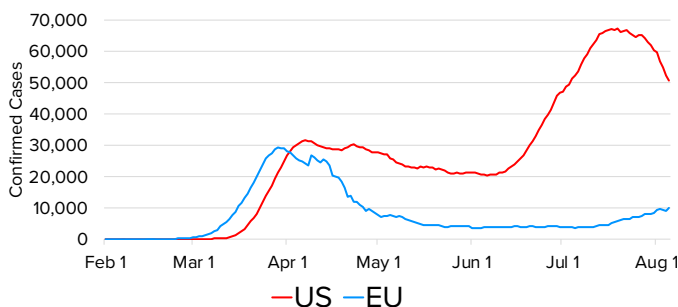
I. DHS Needs to Refocus Its Mission to Lead the Defense of the Nation Against Nonmilitary Threats

Key Findings

COVID-19 in the last five months of 2020 is forecast to kill twenty-five times the number of people killed on 9/11,⁹ and will still be a major threat in 2021.

Pandemic disease has not yet received the leadership attention and resources it deserves. The American people are paying a terrible price. In August 2020, COVID-19 is still ravaging the United States, having killed more than 150,000 Americans¹⁰—more than in the two large flu pandemics of 1967-68 (100,000 dead) and 1957-58 (116,000), or US deaths in World War I (116,516).¹¹ In all of US history, COVID-19 deaths are exceeded only by World War II (US deaths 405,399), the Civil War (620,000), and the 1918-19 Spanish flu pandemic (675,000).¹²

Figure 1: Covid-19 cases in the United States and the European Union



Source: Johns Hopkins University of Medicine (7-day moving average)

In addition to the death toll, COVID-19 has cost the US economy trillions of dollars of lost productivity in what one Nobel Prize-winning economist called a necessary “medically induced coma” that was, nevertheless, not long enough in some states in spring 2020 to bring down infection and death rates.¹³

A faster federal government response to COVID-19 would have cut the death toll by at least half, according to at least

DHS’s Roles in a Pandemic

(DHS abbreviations explained in Annex 1)

Before:

- Develop plans, support training, and run exercises to prepare government officials to deal with pandemics (FEMA, DHS Front Office, PLCY).
- Fund efforts that can help state, local, tribal and territorial governments (SLTT) build resilience against pandemics and other disasters (FEMA).

During:

- Sound the alarm when there is a risk of a pandemic (DHS Front Office, supported by I&A, FEMA, PLCY, Health Affairs, CWMD, CBP, and S&T). Participate in the interagency decision-making to decide how the US government responds (Front Office, PLCY, others).
- Coordinate the response (FEMA), including stockpile and supply chain management. Support the effort using DHS’s authorities and capabilities—disaster response and logistics (FEMA), screening air travelers and those arriving from overseas (TSA and CBP). Provide expertise on infectious disease (S&T through the National Biodefense Analysis and Countermeasures Center (NBACC), CWMD and Health Affairs)
- Support the operational continuity of critical infrastructure, to include modeling and movement of essential workers (CISA, FEMA).
- Provide assistance to foreign partners (All).

After:

- Fund SLTT recovery efforts (FEMA).

Source: DHS web sites, <https://www.dhs.gov>.

one model.¹⁴ Detailed plans written between 2006 and 2016 to respond to a pandemic—commonly called “playbooks”—were not publicized or activated.¹⁵ The Homeland Security Council’s *National Strategy for Pandemic Influenza Implementation Plan* (May 2006),¹⁶ DHS’s own *Pandemic Influenza: Preparedness, Response, and Recovery Guide for Critical Infrastructure and Key Resources* (September 2006), and the Executive Office of the President’s *Playbook for Early Response to High-Consequence Emerging*

Infectious Disease Threats Biological Incidents (2016)¹⁷ could have been activated at an early stage. As Figure 1 makes clear,¹⁸ the difference between COVID-19 cases in the United States and the European Union (EU) points to a massive government-wide policy failure.

The 2002 Homeland Security Act¹⁹ and the National Response Framework of October 2019 both say that the Department of Health and Human Services (HHS) is the lead agency for a pandemic.²⁰ However, DHS has several vital roles to play in responding to a pandemic—all to reduce the number of people affected and to mitigate the economic, social, and security impacts (see box at left). **DHS should take a stronger leadership role in mobilizing resources and public support to defend the nation from COVID-19 and future pandemics.**

Hostile nation-states are increasingly threatening American democracy.

As of January 2021, the most urgent short-term threat to the United States will still be COVID-19. Climate change or extreme weather poses the greatest long-term threat to critical infrastructure in the United States (see Part II below). The next greatest threat to the United States is not terrorism, border security, nor street demonstrations, it is foreign nation-states—specifically Russia, China, and Iran—executing a strategy to weaken the United States by targeting American democracy itself.

Desert Storm (1991), Afghanistan (2001-02), and Iraq (2003) taught American and NATO policymakers the dominance of their military power—but Russia, China, and Iran appear to have learned a very different lesson about the power and capability of non-military campaigns. Author Max Brooks caught the irony of today’s strategic situation:²¹

“Desert Storm was the most disastrous campaign ever fought by the United States—because it taught other countries and non-state actors that

the US military is too powerful to beat on the battlefield and thus must be forced to fight elsewhere. To that end, potential adversaries have been thinking creatively about warfare-by-other-means for decades.”

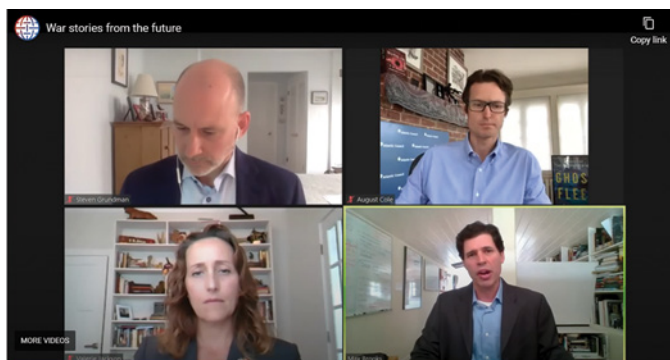
Starting with the 2016 election, and especially once the extent of Russia’s efforts to manipulate the 2016 election became public,²² a consensus emerged among experts in and out of government that a number of American democratic institutions are currently targeted by Russia, China, and Iran.²³ Russia, China, and Iran are carrying out non-kinetic attacks through nation-state cyber operations²⁴ for political or financial gain;²⁵ challenging US election security;²⁶ attacking critical infrastructure;²⁷ carrying out acts of disinformation;²⁸ undermining confidence in the US judicial system;²⁹ manipulating social media, including through foreign covert influence campaigns;³⁰ and using other hostile nonmilitary means to weaken the United States.

While there is no consensus on what to call this—hybrid warfare, gray-zone warfare, active measures, political warfare, or asymmetric warfare—one reason it has proven difficult for the United States to defend against is that it exploits US weaknesses—especially a lack of US strategic patience, political and social divisions, the vulnerability of civilian targets, and the lack of a coordinated defense. And it avoids US strengths, staying intentionally *just below the threshold of triggering a kinetic US military response*—thereby denying the United States a justification to use its unparalleled military power against the nation-states carrying out these attacks. **This strategy is working because it prevents the United States from effective opposition to hostile states’ ambitions while avoiding kinetic war.** Veteran Australian intelligence analyst Ross Babbage in 2019 described the success of Russia’s and China’s approach by quoting the great strategist Sun Tzu, “To win one hundred victories in one hundred battles is not the pinnacle of excellence. To win without fighting is the pinnacle of excellence.”³¹

Russia, China, and Iran, acting more or less independently, share the common goal of weakening US power, and so defense against their non-kinetic methods has to be a much higher US national security priority than it is today.

The fact that these same actors are using similar non-kinetic tactics against other US allies in Europe, the Middle East, and the Asia-Pacific region should make defense against these non-kinetic campaigns one of the United States’ top national security priorities in 2021 and beyond.

On July 24, 2020, William Evanina, director of the US National Counterintelligence and Security Center, issued an extraordinary public warning that China, Russia, and Iran were trying to compromise US political campaigns, candidates, and elections infrastructure, using both social and



Minute 20:30 - 21:30



Inspection of voting machines in North Carolina. At left: DHS Acting Secretary Chad Wolf. Source: DHS photo by Tara A. Molle

traditional media.³² Democrats said even Evanina's stark warning fell short of what the facts required.³³ Former Vice President Joseph Biden on July 17 had raised a comparable warning: "The Russians are still engaged in trying to delegitimize our electoral process. *Fact*. China and others are engaged as well in activities that are designed for us to lose confidence in the outcome."³⁴ Evanina released a stronger "Election Threat Update for the American Public" on August 7, 2020.³⁵

Cyberattacks, threats to election security, threats to critical infrastructure, disinformation, and foreign nation-state threats to confidence in US institutions are, collectively, threats to American democracy itself. The Internet is now an indispensable part of the American economy and the American way of life, as is the nation's critical infrastructure. Elections and free expression are two of the most central aspects of US democracy. Threats to these, especially those that come from hostile nation-states, need to be treated as one of the United States' top national security priorities.

The United States currently has no effective, comprehensive defense against this new style of non-kinetic warfare. Multiple departments and agencies have different roles. While Americans understand that the Department of Defense (DoD) has the lead if there is a shooting war, today **no department "owns" the defense of the United States from non-kinetic cyberattacks against US businesses, state and local governments, or from manipulation of US-based social media platforms to amplify disinformation, or from other foreign efforts to sow division among the American people.** Consider the alternatives:

- Coordination by the **White House** using the traditional interagency process is too slow and cumbersome. Even a White House cyber coordinator would not be

sufficient, because a considerable portion of the effort does not involve cybersecurity. The White House needs to play a coordinating role but does not have an operational capability.

- **DoD** is trained to fight kinetic wars, not to engage in the domestic political arena or the US civilian economy, where most of the attacks in this campaign take place.
- The **State Department** has expertise on international issues, not on domestic infrastructure. Nor does State have the capabilities to defend the United States from these attacks. Diplomacy needs to support the defense of the nation from these threats, not lead it.
- Most of the **Intelligence Community (IC)** focuses on collecting and analyzing foreign intelligence for policy-makers and carrying out presidentially directed covert actions abroad. Many Americans would object to intelligence agencies leading a domestic security effort, and the IC does not have the authority to carry out all the actions inside the United States needed to defend the homeland.
- The **Department of Justice (DOJ)** represents the US government in courts, and houses law enforcement organizations like the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration, and other organizations. But DOJ is neither staffed nor configured to lead the defense of the homeland against this type of attack.
- The **Federal Bureau of Investigation** is configured to investigate crimes, including terrorism, and while its cyber defense and investigative capabilities are strong, the FBI's primary law enforcement mission makes it unsuited to lead a national defense far outside the law enforcement context.

The department best suited to defend the United States against threats to democracy is DHS. DHS is already responsible for much of what is required for a successful defense of the United States—including cybersecurity, critical infrastructure, and election security. As explained in Part II, DHS is already set up to be a conduit for information and collaboration with many of the primary civilian targets of these hostile-nation state campaigns: the US private sector (including social media companies) and federal, state, and local governments.

Even so, **DHS will need more people and resources, and support from other parts of the US government.** DHS will need help in this non-kinetic conflict, just as DoD relies on help from civilian agencies in a kinetic conflict. As former DHS Deputy Secretary Jane Holl Lute often said, there are times when DoD, the State Department, and other parts of the federal government need to think of DHS as the "supported command."

For the defense of American democracy to succeed, the secretary of homeland security and DHS generally will



Members of Maritime Safety and Security Team (MSST) Boston conduct security sweeps of the New York Harbor, Sept. 11, 2014. MSST Boston deployed to Staten Island, N.Y., to assist MSST New York with providing a heightened security presence during the 13th anniversary of Sept. 11. Source: U.S. Coast Guard photo by Petty Officer 3rd Class Frank J. Iannazzo-Simmons

need to be, to the greatest extent possible, nonpartisan and “above politics.” This is essential for credibility on election security. The chairman of the Joint Chiefs of Staff, the uniformed military, and the US Intelligence Community have a similar tradition. Some of the most partisan aspects of DHS’s current responsibilities, like setting the number of immigrant visas, could be given to the White House domestic policy operation or carried out by, for example, establishing separate commissions.

Immigration is currently one such partisan issue, with strong and divergent views held by the major political parties. And DHS involvement in partisan political activities would directly undermine DHS’s more important missions that keep the American people safe.³⁶

While two secretaries of homeland security have come from a background in state politics—a highly relevant consideration given DHS’s need to work closely with state and local governments (see Part II below)—once confirmed, the secretary must be viewed as operating the department in accord with best practices and in a nonpartisan fashion. Former Secretary Janet Napolitano is remembered in DHS for her informal remark that when she became secretary of homeland security, it was as if she had her partisan bone removed—this helped reinforce her serious message, consistent with that of other secretaries of both parties, that what DHS does should be perceived as nonpartisan.

The idea of using a separate commission to deal with controversial issues has succeeded elsewhere, such as monetary policy, which was highly partisan and divisive 125 years ago (e.g., William Jennings Bryan’s “You shall not crucify mankind upon a cross of gold” speech, July 9, 1896). The Federal Reserve Board now sets monetary policy using congressionally approved criteria for full employment, price stability, and moderate long-term interest rates.³⁷ This demonstrates that even hot-button political issues can be de-politicized when there are greater national interests, such as protecting American democracy, at stake.

DHS needs to get ready for the changing terrorist threat.

Any discussion of DHS’s mission needs to include the current state of the terrorism threat to the United States.

DHS has a major role in preventing terrorists from entering the United States, in working with local communities to prevent people from becoming terrorists in the first place—called “countering violent extremism” or “terrorism prevention”—and in working with foreign partners on aviation and border security.

Today, terrorist threats to the United States have changed from what they were immediately after 9/11—and have further evolved from what they were as



Saudi Arabia's Minister of Interior Prince Muhammad bin Nayef bin Abdul Aziz Al Saud greets DHS Counterterrorism Coordinator Under Secretary for Intelligence & Analysis Francis X. Taylor and DHS Deputy Counterterrorism Coordinator for Policy Thomas S. Warrick in Washington, DC, on December 10, 2014. Source: DHS photo by Jetta Disco

recently as 2016. There has not been a large-scale terrorist attack in the United States since 9/11,³⁸ and DHS's aviation and border security efforts are part of the reason why. Al-Qaeda leader Osama bin Laden was killed by US forces on May 2, 2011.³⁹ The Islamic State of Iraq and al-Sham (ISIS) lost control of its final piece of territory in Baghuz, Syria, on March 23, 2019⁴⁰ and ISIS "amir" Abu Bakr al-Baghdadi was killed by US forces on October 27, 2019.⁴¹

The international terrorist threat from the Islamic State of Iraq and Syria (ISIS) and al-Qaeda has not gone away, and DHS needs to use the next two to three years to get ready for what is coming next. ISIS is working on staging a comeback, and is already back to its 2012 level of activity in Iraq.⁴² Bin Laden's successor Ayman al-Zawahiri is reportedly still alive and many of al-Qaeda's adherents moved to other safe havens.⁴³ Al-Qaeda in the Arabian Peninsula (AQAP) claimed credit for the December 6, 2019, terrorist attack at the Naval Air Station in Pensacola, Florida that killed three and injured eight. Terrorist groups are already trying to exploit the COVID-19 pandemic.⁴⁴

Top US military leaders who have led these hard-won US kinetic successes have warned that the United States

cannot capture or kill its way to final victory.⁴⁵ They say the United States needs to move more resources into non-kinetic counterterrorism efforts, especially countering violent extremism or terrorism prevention. For DHS domestically, this means working with communities to prevent people from being radicalized.

For DHS internationally, this means working with the State Department and allies and international partners to implement United Nations (UN) Security Council Resolution (UNSCR) 2396 (2017) to build up worldwide capabilities to disrupt terrorist efforts to travel across international borders. UNSCR 2396 is of special significance for DHS because it was the first time the Security Council established a binding international legal requirement under Chapter VII of the UN Charter that all UN member states needed to install and use aviation security methods that DHS pioneered—especially Advance Passenger Information and Passenger Name Record data (API/PNR)—as well as biometrics and watchlists. DHS had campaigned for years for the universal use of these technologies to make it harder for terrorists and criminals to evade detection when they travel internationally. DHS and the State Department undertook to provide other countries assistance to meet their obligations under UNSCR 2396.⁴⁶



Secretary Jeh Johnson speaks to the media after the Pulse nightclub shooting. Source: DHS photo by Jetta Disco

Domestic terrorism by white supremacists and other “homegrown” causes needs more attention and resources by DHS, the DOJ, and the FBI. Since 9/11, more Americans have died in terrorist attacks by white supremacists and terrorists with similar political alignment than in attacks by ISIS or al-Qaeda sympathizers.⁴⁷ The September 2019 DHS *Strategic Framework for Countering Terrorism and Targeted Violence*⁴⁸ called out white supremacism as “one of the most potent forces driving domestic terrorism.”⁴⁹ But the DHS *Strategic Framework*, which struggled for resources and support since shortly after its release,⁵⁰ has resulted in little visible change in DHS’s actions or priorities.

Recommendations for DHS’s Mission

- 1.1 DHS needs to refocus its mission around today’s most serious threats to the nation: (1) In the short term, COVID-19, which has already killed more than 150,000 Americans⁵¹ and threatens to kill 77,000 more;⁵² (2) starting immediately, nonmilitary threats from nation-states like Russia, China, and Iran; and (3) in the long term, threats to critical infrastructure from climate change or extreme weather.**
- 1.2 DHS needs to lead the defense of the nation on cybersecurity, election security, protecting critical**

infrastructure, countering foreign nation-state disinformation, and countering foreign nation-state misuse of social media—under the mission to “protect American democracy.” Much of what needs defending is in the hands of the private sector, and state and local governments. DHS needs to provide leadership and communication.

- 1.3** While giving greater attention and resources to the threats listed above, **DHS needs to maintain its level of resources and efforts on its existing missions of counterterrorism, aviation security, border management and immigration, maritime security, emergency management, disaster response, and protecting US continuity of governance.** None of DHS’s existing missions is going away.
- 1.4** If DoD’s bumper-sticker version of its mission is “We fight and win America’s wars,”⁵³ **DHS needs to think of its mission as “We lead the defense of the Nation against non-military threats.”** There needs to be clarity—in the White House Situation Room, on Main Street, in Silicon Valley, in the US Congress, and among DHS’s own employees—which cabinet department leads the defense of the nation against the non-kinetic campaigns now being waged by nation-states determined to undermine US power.⁵⁴

Three urgent recommendations to address COVID-19:

- 1.5 DHS needs immediately to devote significantly greater leadership focus and resources to efforts against COVID-19.** COVID-19 is far and away the greatest, most urgent short-term threat to the security of the United States—with the potential to inflict additional American deaths equal to twenty-five more 9/11 attacks before the end of 2020.⁵⁵ DHS needs to do much more to harmonize states' response efforts and to solve the COVID-19 resource and logistic shortfalls that continue to occur across the nation, six months after the scope of the pandemic became clear. **DHS should mobilize and prioritize the increased, coordinated distribution of needed testing, vaccination and medical supplies, and the infrastructure changes required to make US schools, factories, nursing homes, and offices safe.**
- 1.6 DHS should be more proactive in sounding the national alarm in future pandemics and public health emergencies, to ensure the federal government is fully mobilized.** The failure to mobilize the federal government and provide leadership across the homeland security enterprise for a unified, national effort in January and February 2020 resulted in tens of thousands of avoidable deaths in the United States. This should never happen again. Even though HHS has the lead in public health issues, if the secretary of HHS cannot organize the necessary support, DHS should do more to mobilize the response to global and domestic health emergencies. DHS has the ability that HHS does not to elevate a public health issue into a national security issue.
- 1.7 DHS likewise should ensure that national medical supply stockpiles are rebuilt quickly and that pandemic plans and playbooks are kept available so they can be publicized, activated, and executed when needed.** DHS needs to speak out more forcefully and publicly about the reason for the appropriations requests to replenish the national stockpiles, because this is a national security issue in addition to a public health issue. Experienced White House veterans know that in a change of administrations, it is not just personnel who are changed—White House computer systems are erased. Both of these can leave a gap in institutional knowledge about emergency planning for pandemics and other infrequent, high-consequence events such as earthquakes. Because of DHS's responsibilities in emergency management and planning for the federal government, DHS should have both the responsibility and the capability to recall and make known playbooks and other plans for addressing contingencies like pandemics. This should include the ability in an emergency to activate planning without waiting for formal instructions.

- 1.8 DHS needs additional resources for both cybersecurity and election security and should submit an emergency supplemental request for the Cybersecurity and Infrastructure Security Agency (CISA) in the first half of 2021** to deliver help in time for the November 2022 election. The US Cyberspace Solarium Commission has also called for additional resources for DHS cybersecurity.⁵⁶
- 1.9 The next DHS leadership team needs to be built around a common understanding of the most urgent threats to the nation outlined in Recommendation 1.1. DHS must move away from the current decentralized approach in which component leaders often set their own priorities.** A department where the component leaders set their own priorities will not succeed.

Two urgent recommendations for communications and public engagement:

- 1.10 Communications is a core DHS mission. DHS requires world-class capabilities to communicate much more effectively with the American people, DHS stakeholders in the private sector and state and local governments, and, especially, DHS's employees.** DHS needs a public affairs, internal communications, and a legislative affairs operation to match those of the State and Defense Departments. DHS leadership also should do more to listen, because DHS needs information from its stakeholders and employees to succeed. DHS's communications professionals need to be involved early in the policy making process to advise on effective communications with the public and other stakeholders, and to be able to report candidly to policy makers when policies are not working or are not understood by the public.
- 1.11 DHS also needs to invest urgently in considerably wider access to classified voice and data networks used throughout the national security community.** Other national security agencies including State, the Department of the Treasury, DOJ, and the FBI make widespread use of classified voice and data systems to protect national security information. If DHS is to lead the defense of the nation against non-military attacks by highly sophisticated nation-states like Russia and China, DHS needs wider availability of classified voice and data networks.
- 1.12 DHS, more than other cabinet departments, needs to factor into its decisions how its actions affect the trust the American people have in DHS.** DHS needs the support of the American people in order to succeed.⁵⁷ DHS relies on voluntary cooperation

and the sharing of information from state and local governments, and from the private sector, to protect computer networks and critical infrastructure. Even security functions like aviation security rely on the American people accepting what DHS does as necessary for their protection. The public needs to have confidence that the information they provide to DHS is used appropriately—a consideration that will become even more important as technologies like facial recognition become more widespread than they are at present. Stories of aggressive pat-downs at airport checkpoints of grandmothers, small children, or people with disabilities hurt DHS’s ability to do its mission. Public confidence in DHS cannot be commanded; it must be earned whenever DHS takes action.

A Pew Research Center study released in April 2020 said that the American people held a favorable view of DHS by 71 percent vs. 24 percent unfavorable—but for Immigration and Customs Enforcement (ICE), the numbers were split 46 percent favorable vs. 45 percent unfavorable.⁵⁸ While security should not necessarily be governed by opinion polls, the American people and their state and local governments need to be assured that DHS will exercise its authorities responsibly. DHS needs to re-think both its overall approach to immigration enforcement and its recent policy of arrests in the streets away from federal buildings it is authorized to protect. DHS offices such as Civil Rights and Civil Liberties (CRCL) and Privacy (PRIV), which directly report to the secretary, are important in this regard.⁵⁹ Americans have a visceral negative reaction to federal officers in desert camouflage and gas masks using their powers aggressively in the streets of the United States. It is vital to DHS’s mission that DHS find ways to deal with the use of information, immigration enforcement, and protec-

tion of federal property in ways that do not alienate states, cities, and the American people.

1.13 Expecting the unexpected needs to be a normal, permanent part of DHS’s mission. DHS should have both the authority and the ability to shift focus, money, and people more rapidly than at present. DHS’s mission will always involve responding to events that were unforeseen or exceeded what was foreseen. Because of DHS’s responsibility for disaster response, and because of DHS’s broad mission space, popular opinion associates DHS with events like Hurricane Katrina (2005), Deepwater Horizon (2010), Hurricane Sandy (2012), the southwest border crises of 2014 and 2019, and COVID-19 (2020). This is true even for those crises that the experts foresaw but for which the government was not adequately staffed and resourced when the crisis hit. **DHS needs to be able to meet the challenge not just of predicting what might go wrong, but to operationalize and pre-plan the response so that DHS can turn what would otherwise be a major disaster into a lesser, manageable one.**

1.14 The secretary of homeland security should become a statutory member of the National Security Council. Although National Security Presidential Memorandum no. 4 and its predecessors made the secretary of homeland security a member of the National Security Council, by law the mandatory members of the National Security Council are only the president, the vice president, the secretary of state, the secretary of defense, the secretary of energy, and the secretary of the treasury.⁶⁰ The secretary of homeland security is the only cabinet official with broad national security responsibilities who is not yet a statutory member. This recommendation will take congressional legislation to implement.

II. DHS's Public-Private Partnerships Are Unique and Should Be Modernized to Effectively Counter the Threats of the 2020s

Key Findings

Protecting American democracy and building a resilient homeland is a shared endeavor across a diverse set of stakeholders known as the homeland security enterprise (HSE). This fundamental principle distinguishes DHS's mission from that of other cabinet departments. DHS has the unique ability to bring others together to solve a crisis or avert a threat. While DHS may lead or direct specific operations, DHS's chief responsibility is often to coordinate efforts of federal departments and agencies, in consultation with state, local, tribal, and territorial (SLTT) governments, nongovernmental organizations, private-sector partners, and the public, a partnership commonly referred to as the "homeland security enterprise." DHS should not be viewed at the top of a pyramid directing downwards—if anything the "pyramid" is inverted with DHS often in a supporting role or called upon to assist when partner resources are overwhelmed and they ask for federal assistance.⁶¹

The enormity of the homeland security mission can be appreciated by the scale of American geography and political economy: Alaska is about the geographical size of Mexico, and if California were a country it would be the fifth largest economy in the world. Adjacent US states do not always share the same natural hazards or perceived terrorist targets. American industry owns and operates the majority of the assets, systems, and networks that underpin the American way of life, the continuity of the economy, and US national security. Building a safe, secure, and resilient nation requires a harmonized approach to managing strategic risk and defending against threats from nation-states, terrorists, and criminal adversaries. In this environment, trust, communication, information sharing, and shared understanding of desired outcomes are essential.

Homeland security is a decentralized enterprise shared by diverse stakeholders in the public and private sector. While DHS is the lead federal partner in the execution of the homeland security mission,⁶² managing strategic risks—including defending against the threats discussed in Part I of this report—requires a collaborative and inclusive effort among various partners in the homeland security enterprise. The first Quadrennial Homeland Security

Review presented homeland security "as a distributed system, where no single entity is responsible for or directly manages all aspects of the enterprise."⁶³

While DHS may lead and direct specific operations, DHS's chief responsibility is often to coordinate efforts of executive departments and agencies, in consultation with SLTT governments, nongovernmental organizations, private-sector partners, and the public. DHS often finds itself in a supporting and consultative role or called upon to assist when the resources of a partner are overwhelmed and federal assistance is requested.⁶⁴

As the COVID-19 response showed, if partners take divergent approaches to strategic and existential threats, it can undermine the national effort. For example, when DHS failed to coordinate both procurement and distribution of scarce personal protective equipment (PPE) during the pandemic's early days, it created a bidding war among the states, prompting prices to soar to the detriment of those who needed PPE.⁶⁵ It also exacerbated supply chain uncertainty and paralyzed the mutual aid system between jurisdictions. Cyberattacks on infrastructure, election disinformation campaigns, and climate change or extreme weather all have regional or national effects, and yet must be defended one building or computer network at a time.

DHS is distinct among federal agencies in the kinds of relationships it has with the private sector. Each relationship is unique to the mission, governed by different statutes and authorities. DHS's relationships fall into these categories:

- **Operational** — For example, the Transportation Security Administration (TSA) works with airlines and airports to adjust procedures to meet evolving security threats.
- **Operational Support** — For example, the Federal Emergency Management Agency (FEMA) works after disasters to remove physical and bureaucratic obstacles to private sector recovery efforts, so people can rebuild their lives and the economy can recover.
- **Supporting** — For example, CISA shares threat and vulnerability information with industry so that corporate security programs can defeat threats and mitigate risk.



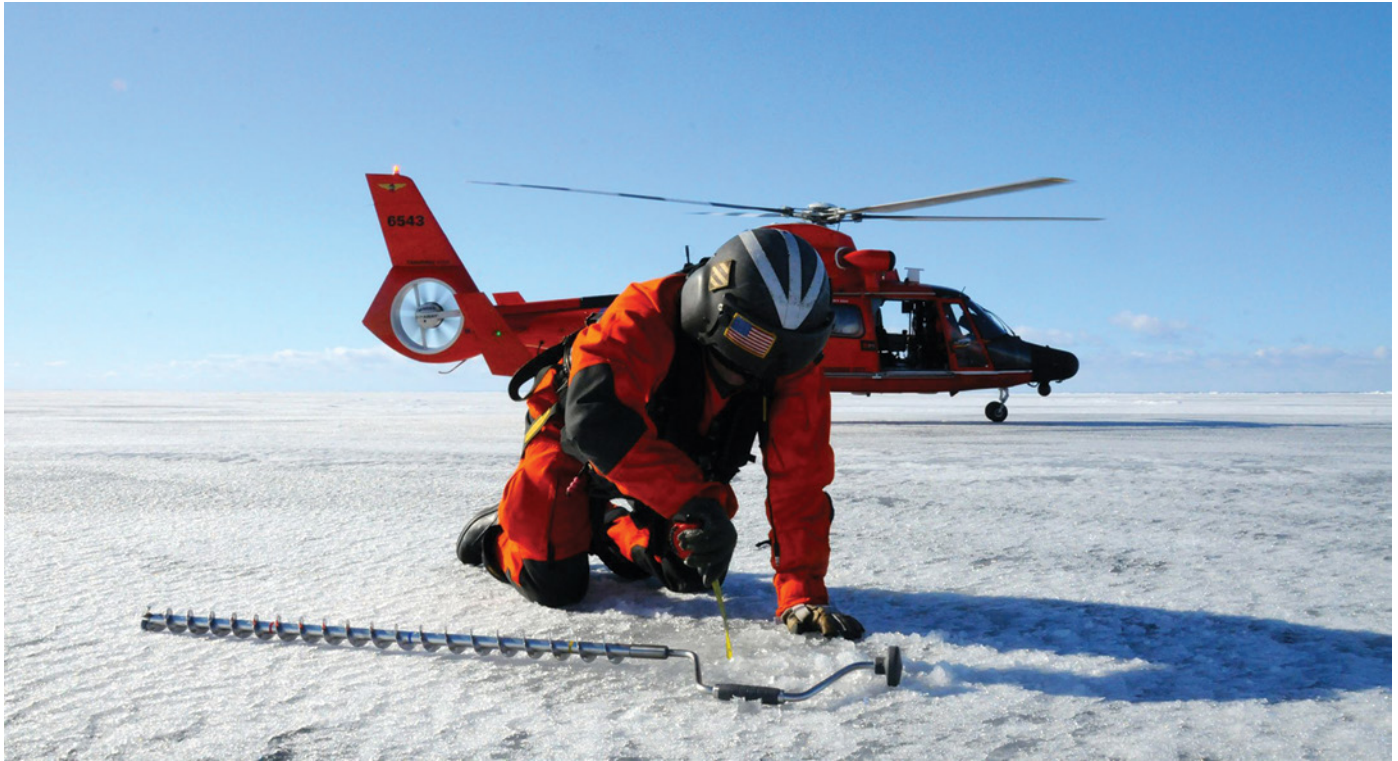
Secretary Jeh Johnson meets with state officials in Baton Rouge, LA. Source: DHS photo by Barry Bahler

- **Regulatory** — For example, the US Coast Guard (USCG) and CISA chemical security regulations focus on maritime and chemical industry facilities that have a higher-than-average risk for security incidents.
- **Contractual** — Like other departments and agencies, DHS contracts for integrated logistics support or advanced systems and technologies for DHS's front-line employees.

DHS's ability to foster information sharing between private-sector companies, some of which compete with each other, is a vital reason why the homeland security enterprise is essential. DHS's information sharing programs are designed to let companies facing similar threats share situational awareness about those threats. DHS's information sharing exposes cyber vulnerabilities and hostile exploits, for example, which allows other companies to defeat threats and avoid risk that, without DHS, would likely defeat them one at a time. Authorities such as the Cyber Information Sharing Act of 2015⁶⁶ and Protected Critical Infrastructure Information⁶⁷ encourage the two-way sharing of information by allowing private businesses to share information about

vulnerabilities, exploits, or incidents. DHS does this by providing liability and other protections when companies share information in DHS-approved channels. Similarly, the supply chain security efforts of Customs and Border Protection (CBP), including the Customs-Trade Partnership Against Terrorism (C-TPAT) and the CBP-TSA Air Cargo Advance Screening program (ACAS) are proven mechanisms for the private sector to share supply chain and other vulnerabilities with DHS, which allows DHS and the private sector to enhance supply chain security and resilience.

Most often, the sharing of unclassified or downgraded classified information on hostile tactics or techniques enables corporate security or cybersecurity officials to share information within their organizations. **Stakeholders such as the financial services, telecommunications, and electricity sectors, need higher-fidelity, often classified, intelligence to take action.** This lets businesses make informed decisions and take actions to mitigate threats. **Increasing the speed of sharing is now vital, as cyberattacks happen at network speed, and the federal government needs to be able to communicate relevant information,**



Coast Guard crew member measuring ice thickness. *Source:* U.S. Coast Guard photo

including attribution, in real-time to enable companies to prevent damage to their systems or the theft of valuable information.

Foreign adversaries are already carrying out attacks on US critical infrastructure. As evidenced by a July 23, 2020 National Security Agency (NSA) and CISA joint Cybersecurity Alert,⁶⁸ nation-state adversaries conduct malicious activity against critical infrastructure, often exploiting Internet accessible operational technology. While foreign nation-state cyberattacks against critical infrastructure have risen exponentially over the last ten years, infrastructure can also be the target of kinetic attacks, including by violent extremists.

Climate change or extreme weather represents the most significant long-term threat to critical infrastructure. Climate change will also have an increasing impact on the operational environments that DHS helps secure. DHS is not responsible for addressing climate change, but it is responsible for getting partners to protect the infrastructure that is at risk due to climate change or extreme weather. DHS will need to help organize and support the state, local, and private sector investments to develop the necessary resilience to climate change and associated trends.⁶⁹ Famine or drought can drive mass migration in Central America or cause terrorists to relocate

from a safe haven overseas to the United States or our allies. Melting sea ice is a reality for the USCG in the Arctic that could lead to new opportunities for shipping, tourism, and legal resource exploration, but also for illegal smuggling and trafficking, environmental disasters, and illicit resource exploitation—in today's world economy, fisheries are a vital national resource.

Climate change is driving the frequency, size, impact, and complexity of a range of natural disasters, including storms, floods, droughts, and wildfires. This places additional resource requirements on FEMA. As these disasters become more complex, their cascading effects become more unpredictable, and thereby stress the entire homeland security enterprise. Higher temperatures and more intense storms may also damage or disrupt telecommunications and power systems, creating cascading consequences for telecommunications infrastructure, emergency communications, and cyber system failure. While FEMA's Build Back Better public assistance program⁷⁰ provides funding to mitigate future disasters, DHS needs an enterprise-focused climate change strategy to address the entirety of its ecosystem. Equally important, the security implications of climate change must be addressed in any comprehensive climate change plan. DHS must have a seat at the table to ensure DHS's missions and the equities of DHS's stakeholders are understood.

Recommendations for Modernizing DHS's Public Private Partnerships

Overall

2.1 Task the Office of Partnership and Engagement (OPE) with developing a comprehensive engagement strategy to increase trust and harmonize engagement with key private sector partners and make better use of convening authorities. DHS's engagements with the private sector have grown, often without sufficient planning on how to leverage those relationships across the department. Senior-level engagement with the private sector, especially corporate leadership, should be continuous and collaborative so that when new or urgent issues arise, senior officials do not find themselves trying to build trust for the first time. As noted above, DHS needs to develop trust to be effective in working with partners across the homeland security enterprise.

While CISA carries out many of these engagements, so do other parts of DHS. The Office of Partnership and Engagement reports directly to the secretary and is the right office to develop a comprehensive strategy and a plan to overcome the constraints and obstacles that are preventing DHS from engaging in substantive dialogue with industry in order to allow industry to better protect itself.

DHS has unique authorities to convene government and private sector stakeholders to address active and emerging threats. DHS's incoming leadership does not always know or appreciate these authorities. Understanding the extent and applicability of these authorities can aid the secretary and headquarters staff in identifying courses of action that mitigate threats in a crisis.

These authorities, when used appropriately, allow department leadership to have substantive discussions with industry that would normally be constrained by federal acquisition and government ethics rules. The secretary of homeland security can privately seek advice and counsel from a company or an industry, for example, to close a security gap that terrorists or hostile nation-states would otherwise exploit.

Additionally, DHS knows that engagement must be continuous and collaborative, not episodic or directed, but this takes strategic planning because senior DHS and corporate leader attention must be reciprocal, so that when new or urgent issues arise, senior officials do not find themselves trying to build trust



Assistant Secretary Caitlin Durkovich at a DHS-led active shooter workshop. Source: DHS photo by Barry Bahler

for the first time. Nor should relationships be constrained by one individual on either side feeling he or she “owns” the relationship. A strategy will help DHS senior leaders maximize DHS's ability to interact with the private sector in ways that strengthen the security of the homeland.

2.2 DHS should inventory its information-sharing relationships and adjust its practices according to the different levels and capabilities of SLTT and private sector stakeholders. Information sharing is not one-size-fits-all, and DHS needs to adjust its practices accordingly. When DHS shares information, it should be both timely and actionable. Different-sized organizations have different levels of sophistication and need different levels of detail to drive corporate executive actions. Large firms, or companies in technically sophisticated industries such as telecommunications and financial services, already have a high level of knowledge. Sometimes they need very specific and actionable information, often at a classified level, to drive executive action. Some companies just want to be told what DHS needs them to do.

DHS headquarters needs to have a comprehensive understanding of its various information sharing relationships and those of other federal departments and agencies. The secretary should direct an inventory of DHS's different information sharing programs, their purpose, and their perceived utility to stakeholders. The deputy secretary should convene regular meetings with the Office of Strategy, Policy,

and Plans (PLCY), Office of Intelligence & Analysis (I&A), Office of Public Affairs (OPA), Office of Partnership & Engagement (OPE), Office of Legislative Affairs (OLA), and component programs to coordinate messaging and two-way information sharing on emerging threats to ensure information is shared at the appropriate classification level—as much of it as possible to components in the field at the unclassified level. Given the failure before 9/11 to connect the dots—which appears to have happened in the early months of the COVID-19 pandemic—DHS needs to enhance its information-sharing and data visualization programs.

2.3 DHS should devolve operational-support decisions to the local level to strengthen trust with SLTT partners—and have DHS’s local representatives communicate to headquarters what they are hearing. DHS is collectively the largest “retail” face of the federal government to the private sector. To many private sector partners, DHS is locally based. DHS components are distributed across the country and employees work locally to help secure ports, waterways, critical infrastructure, to include soft targets. DHS needs to do more to take advantage of its sustained, retail presence, which is often better attuned than Washington to the needs of local partners. DHS leadership should institutionalize a process, to include regular visits to the field, whereby field employees can report and share their observations with headquarters and in turn, policies and programs can be tailored to address and support the unique needs of the stakeholders.

2.4 DHS should designate “systemically important critical infrastructure” and DHS’s support should be comparable to what DoD provides to the companies in the defense industrial complex. DoD’s Defense Industrial Base (DIB) is an unmatched element of US national power that differentiates the United States from all potential opponents by allowing DoD to draw on what the private sector can build in times of national emergency or crisis.⁷¹ DHS needs to develop a comparable relationship with “systemically important critical infrastructure” that underpins our democracy, economy, and national security. The US Cyberspace Solarium Commission recommended that Congress should codify the concept of “systemically important critical infrastructure” so that entities responsible for systems and assets that underpin national critical functions receive additional security support from DHS consistent with their critical status and importance.⁷² DHS should also determine whether to implement mandatory cyber incident reporting for “systemically important critical infrastructure” analogous to the DIB requirements.

2.5 Make threats against critical infrastructure a priority across the Intelligence Community. The secretary should work to ensure that the US Intelligence Community’s collection priorities include changes to threats against critical infrastructure companies. A May 2018 report of the Council of Foreign Relations rightly pointed out that the federal government’s classified information sharing program with the private sector is a system of a bygone era and that the government needed to give increased priority to collecting intelligence on threats to private companies, particularly critical infrastructure operators, and amend its processes for disseminating that intelligence.⁷³ The National Infrastructure Advisory Council similarly recommended that Threats to Critical Infrastructure should be a Priority 1 topic within the National Intelligence Priorities Framework.⁷⁴ A validation process would be needed to ensure transparency and that collection requests are used only for the purposes of protecting infrastructure against threats to national and economic security. This will work only if the private sector trusts what DHS is doing.

Climate change or extreme weather

2.6 DHS should incentivize efforts to enhance resilience and mitigate risk, in addition to supporting crisis-driven response activities. Studies show that mitigation projects can avoid as much as \$6 in damage for every \$1 invested.⁷⁵ As the United States’ threat profile shifts away from foreign terrorist attacks on US soil toward pandemics; nation-state threats to democracy; natural disasters like hurricanes, storms, and earthquakes; as well as climate change or extreme weather; cyberattacks; and the other threats of today, DHS’s grant programs should adapt as well. For example:

- At least 50 percent of the annual \$1 billion Homeland Security Grant Program (HSGP) should be reserved for all-hazard threats, including counterterrorism, cyberattacks, pandemics, and other “nontraditional” threats.
- As extreme weather, cyberattacks, and other asymmetric threats increasingly penetrate the risk landscape, DHS should advocate for adapting the national network of fusion centers, which are largely funded by HSGP, from a law enforcement-centric approach to an all-hazards framework. Such a shift in approach ultimately lies with state and local partners, but would better support the department’s mission to build resilience to all hazards.
- FEMA should adapt the Hazard Mitigation Grant (HMG) and Building Resilient Infrastructure and Communities (BRIC) programs to incentivize SLTT partners to undertake projects that build resilience against climate change, pandemics, cyberattacks,



Members of Coast Guard Shallow-Water Response Boat Team 3 help pets stranded by floodwater caused by Hurricane Florence, North Carolina, Sept. 16, 2018. *Source:* U.S. Coast Guard

and other “non-traditional” threats—breaking out of its traditional, narrow emphasis on floods and storms.

The importance of these very significant grant programs suggests they might fare better outside of FEMA, in a DHS component that is more policy-oriented and less operationally focused.

Moreover, the Office of Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act Implementation, which provides “liability protections to companies that develop and deploy anti-terrorism technologies,” should be moved out of the Science and Technology Directorate (S&T) and placed within CISA to better align with the critical infrastructure risk management mission. Owners of critical infrastructure assets are increasingly seeking certification, which allows them to display DHS approved SAFETY Act marks, akin to a “Good Housekeeping Seal of Approval.” The SAFETY Act provides one of the strongest incentives to the private sector to use their own resources to make the United States more secure.

Cybersecurity

2.7 DHS should work with Congress to authorize and appropriate a Cyber Resilience Fund, akin to the Disaster Recovery Fund, to support rapid response and recovery of national critical functions. In a crisis, there is no substitute for ready cash, and this is espe-

cially true if a nation-state adversary takes down a major part of US critical infrastructure. If DHS is going to deter and defend against the type of warfare that US adversaries are now waging, DHS needs to be able to demonstrate that the United States can rapidly restore critical functions across corporations and industry sectors and get the economy back up and running. Nothing undermines an adversary’s cyber offensive strategy better than a recovery that happens within hours rather than days. This was a recommendation of the US Cyberspace Solarium Commission.⁷⁶

2.8 DHS should support and lead the Joint Collaborative Environment, a common and interoperable environment for the sharing and fusing of threat information, insights, and other data across the federal government and between the public and private sectors. Data need to be shared or cross-correlated at the speed and scale necessary for rapid cyber threat detection and identification. This was also a recommendation of the US Cyberspace Solarium Commission.⁷⁷

2.9 The White House should establish a national cyber director in the Executive Office of the President, at the level of assistant to the president, and **give the CISA director a seat at the Deputies Committees alongside the DHS representative**—just as both the under secretary of defense for policy and the vice chairman of the Joint Chiefs of Staff sit at the deputies’ table when the military defense of the nation is being discussed. The reasons are analogous. Military expertise needs to have a voice at the table, not just as a backbencher, when policy decisions about the use of force are decided. Similarly, cybersecurity expertise needs to have a voice at the table when the United States makes policy decisions about how to defend against nation-state, terrorist, or even criminal enterprise cyberattacks.

It is also important for **DHS and CISA to be at the table when decisions are made about US offensive cyber operations, even the most sensitive when most other cabinet departments are excluded from the decision-making process.** A tactic, software tool, or method of attack used by US offensive cyber operators can be turned against the United States in a matter of hours or days. DHS needs to be able to caution other policy makers if the United States has particular vulnerabilities to the same attack method—offensive cyber operators might not know the vulnerabilities of US cyber infrastructure operators. Additionally, DHS may need time to prepare US cyber defenses so that US cyber infrastructure operators can defend themselves when the tactic is turned against them. Recent history is replete with examples



CBP AMO agents deliver food and water to severely damaged Fox Town on the Abaco Islands in the Bahamas, in the aftermath of Hurricane Dorian Sept. 6, 2019. Source: CBP photo by Kris Grogan

where US offensive cyber tools were disclosed and turned against targets inside the United States.⁷⁸

Other recommendations

2.10 DHS should build the capacity to identify emergent, strategic threats—and the capabilities that will be needed to counter those threats. DHS needs to shift to a more anticipatory, proactive risk mitigation model, and it should work to ensure its stakeholders do also. DHS Science & Technology (S&T) should be restructured to provide foresight and strategic thinking about how threats are evolving and what the technology for tomorrow needs to be across the HSE. S&T's focus should be on early and emerging technologies and technological solutions. S&T will need to consult more closely, not just with DHS's operating components, but also with other parts of DHS responsible for forward thinking on issues like terrorism, cyber-threats, threats to large data systems, and even upcoming legal challenges to management of data.

2.11 DHS should strengthen trust with its partners across the homeland security enterprise. More than almost any other part of the federal government, DHS needs the support of its stakeholders to succeed. Trust is the foundation of DHS's information sharing and risk management activities. DHS relies on voluntary cooperation from state and local governments and the private sector to protect everyone's computer networks and critical infrastructure. Certain missions and partnerships—most notably those of CISA and TSA—have so far been immune to the fallout from recent DHS missteps and operational blunders, but even these are going to be at risk unless DHS increases the priority of strengthening trust.⁷⁹ To build trust, DHS components must sit across the table from their private sector partners, communicate regularly, ensure there is a shared understanding of the problems, speak of the value of mitigating risks in language that private sector partners understand, and demonstrate a return-on-investment or other measures of success.

III. Resolving the Issues That Cause DHS's Low Morale

Key Findings

When large cabinet departments are ranked by overall morale, DHS has occupied last place every year since 2010. Other departments go up and down over the years (see Figure 2), but DHS has been last in twelve out of thirteen surveys done since 2003. Yet at the same time, DHS employees remain committed to the department and its missions. **Addressing the workplace issues that drive DHS's low morale needs to be one of the top priorities that DHS's leadership team should address.** Sustained leadership attention to the specific workplace issues, especially at TSA and CBP, could allow DHS to considerably improve overall morale over the next two to four years.

Measuring morale. Each year, the Office of Personnel Management conducts the Federal Employee Viewpoint Survey (FEVS),⁸⁰ asking the civil service workforce about a hundred questions about their views on their workplace. The Partnership for Public Service's "Best Places to Work in the Federal Government" project makes the data more broadly accessible.⁸¹ The Partnership weights the answers to three specific questions that, over time, have been able to predict whether an employee will remain with the agency.⁸²

While the FEVS survey reports that morale at DHS is low, the FEVS survey also shows that DHS employees remain committed to the department and its missions. **DHS's best FEVS score relative to other departments is "The work I do is important."** Upon hearing that the Atlantic Council was undertaking this study of how to improve DHS, more than a hundred current and former DHS officials volunteered ideas and recommendations. The following comes from an analysis of the FEVS data.

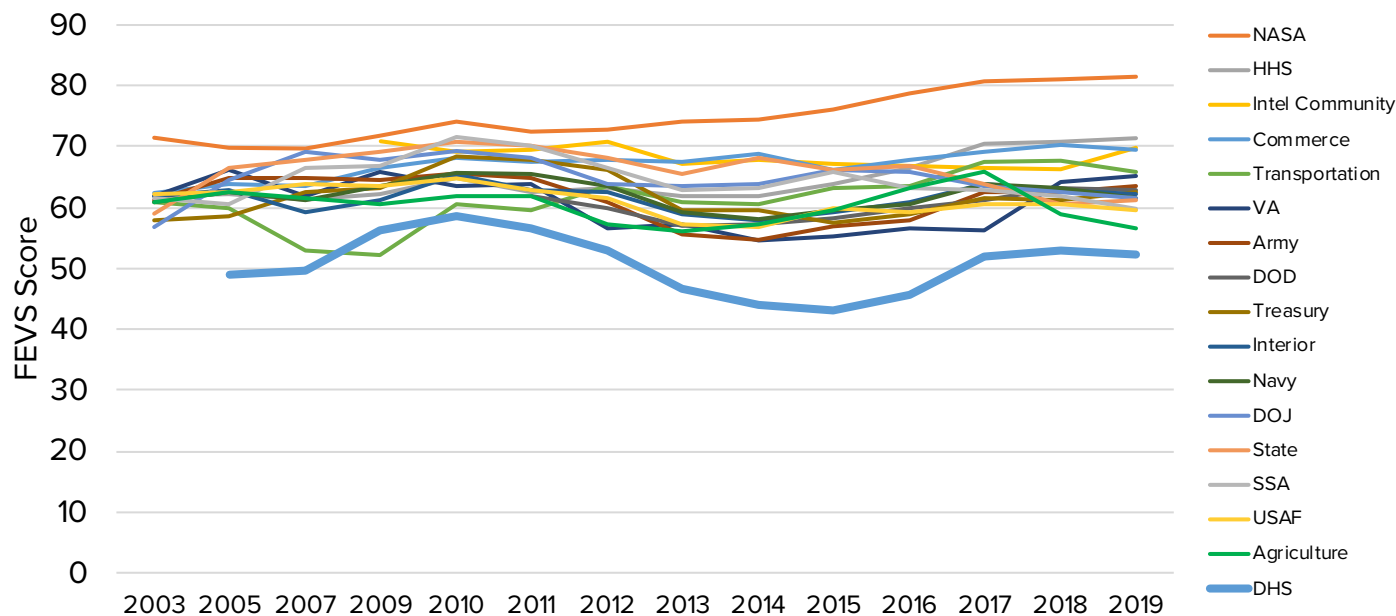
DHS is a component-driven organization, which hinders the department's ability to fully align employees to a unified mission and shared purpose. Efforts to build a "One DHS" or "Unity of Effort" model were not sustained long enough or deep enough to take root. As a result, DHS today still lacks an overall unifying, organizational culture. Employees feel a stronger loyalty to their component and almost no loyalty to the department as a whole.

The lack of a common DHS organizational culture and other challenges related to different degrees of employee engagement are holding DHS back from moving toward an organizational culture of innovation, collaboration, and empowerment. FEVS survey data show a



DHS employees at a town hall meeting. Source: DHS photo by Jetta Disco

Figure 2: Results of Federal Employee Viewpoint Surveys (FEVS) by cabinet department



Source: Partnership for Public Service, *Best Places to Work in the Federal Government, 2019*

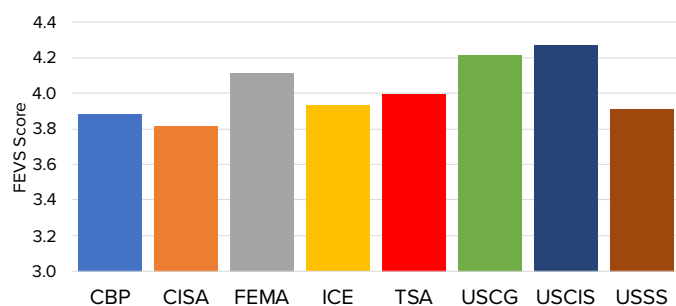
widespread perception of a “punishment culture” and a “culture of no” where potential solutions are not always voiced, success is not consistently celebrated, and employees’ personal empowerment is not always clearly defined. In 2019, only 41.2 percent of DHS respondents agreed employees have a feeling of personal empowerment with respect to work processes—compared to 50 percent government-wide. In 2019, only 44.7 percent of DHS respondents agreed employees are recognized for providing high quality products and services—compared to 54 percent government-wide. DHS’s score on FEVS question thirty-two, whether “creativity and innovation are rewarded,” is one of the lowest-scoring questions across the entire department.

DHS employees are focused on their component’s goals and appear not to know or understand about departmental strategies or goals, nor how their individual work contributes to the larger DHS mission. On FEVS question fifty-six, “Managers communicate the goals of the organization,” DHS employees ranked the department fourteenth out of fourteen—lowest ranked of the large cabinet departments for which FEVS reported data. In contrast, DoD briefs national strategies, such as the Defeat-ISIS strategy, down to the battalion commander level.⁸³

On FEVS question twelve, “I know how my work relates to agency goals” (Figure 3), US Citizenship and Immigration

Services (USCIS) and US Coast Guard (USCG) employees—13 percent of the department—rate DHS highly. But CBP, CISA, Immigration and Customs Enforcement (ICE), TSA, and the US Secret Service (USSS) employees—74 percent of DHS—have less of an understanding of how their work relates to agency goals. In 2019, only 51 percent of DHS respondents agreed that “Managers review and evaluate the organization’s progress toward meeting its goals and objectives,” compared to 64 percent government-wide.

Figure 3: Response to FEVS Question 12 by DHS component, 2017-19 3-year average, “I know how my work relates to agency goals”



Source: Office of Personnel Management, FEVS, *Report by Agency*

Table 1
DHS Employees by Component, 2018

	Employees	Percent
TSA	64,051	30.76%
CBP	60,524	29.06%
FEMA	19,920	9.57%
ICE	19,912	9.56%
USCIS	18,738	9.00%
USCG	8,530	4.10%
USSS	7,292	3.50%
DHS HQ	3,397	1.63%
CISA	3,295	1.58%
FLETC	1,248	0.60%
OIG	760	0.36%
S&T	408	0.20%
DNDO	179	0.09%
Total	208,254	100.00%

Source: Office of Personnel Management, *Fedscope*

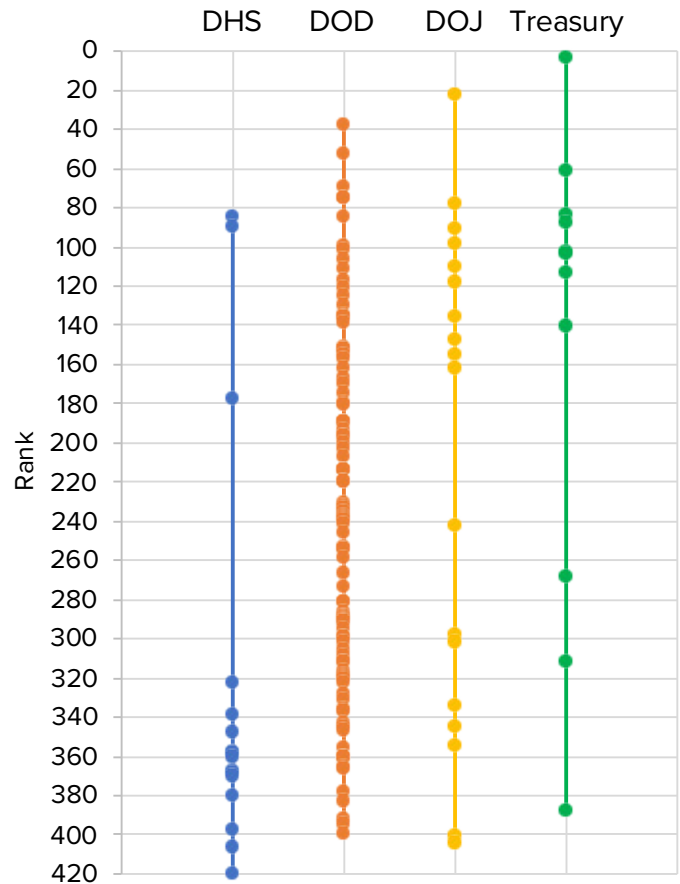
Survey results show that trust between DHS employees and senior department and component leaders is low. Improving employee trust has to be central to DHS's workforce and morale strategies. It must be noted that the FEVS questions are ambiguous as to whether “senior leaders” refers to DHS leaders or component leaders. It is also clear that responses to specific questions tend to move up or down together, suggesting that DHS employees reward or punish their leaders across the board, raising all scores when things improve, but giving everything lower scores when morale declines.

In 2019, only 37.7 percent of DHS respondents agreed that “In my organization, senior leaders generate high levels of motivation and commitment in the workforce,” in contrast to the government-wide score of 45 percent. In 2019, only 47.9 percent of DHS respondents (compared to 56.1 percent government-wide) agreed that “My organization's senior leaders maintain high standards of honesty and integrity.” This is remarkable in a department with the missions and functions that DHS has.

Turning around DHS's morale problems starts with the two components that drive the department's low FEVS scores: TSA and CBP, which together account for more than 59 percent of DHS's employees (Table 1).⁸⁴ DHS's overall score is weighted by the number of employees (survey respondents) in each component.

As Leo Tolstoy wrote in the opening sentence of *Anna Karenina*, “All happy families are alike; each unhappy family is unhappy in its own way.” That applies to DHS's

Figure 4: FEVS rankings of subagencies, 2019



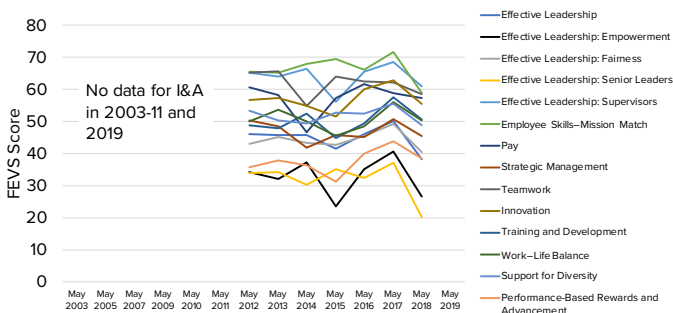
Source: Partnership for Public Service, *Best Places to Work in the Federal Government*, 2019

components. Specific recommendations address TSA and CBP below.

The United States Coast Guard (USCG) and US Citizenship and Immigration Services (USCIS) consistently rate highly compared to all federal subagencies, but unlike DHS's closest counterparts—DoD, DOJ, and Treasury—most DHS components are clustered at the bottom (Figure 4). DHS's Countering Weapons of Mass Destruction office (CWMD) was the lowest-ranking subagency in the federal government in 2019, ranking 420 out of 420. CWMD's assistant secretary was removed in October 2019⁸⁵ and replaced by DHS managers with decades of experience at TSA and USCG.⁸⁶ This is an important positive example because, as will be shown later, removing poor performers is something DHS needs to do more of.

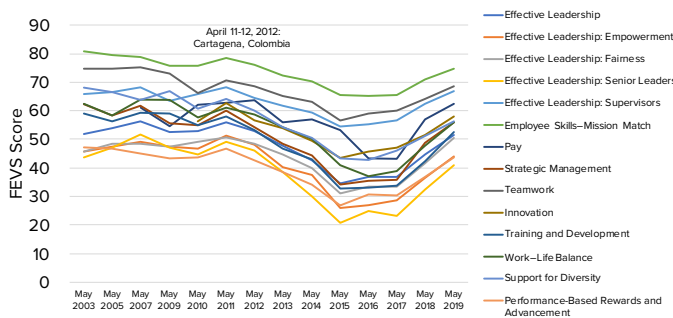
DHS has had some remarkable success stories in turning around employee morale that should be recognized, understood, and where possible replicated.

Figure 5: DHS's Information & Analysis FEVS scores by category



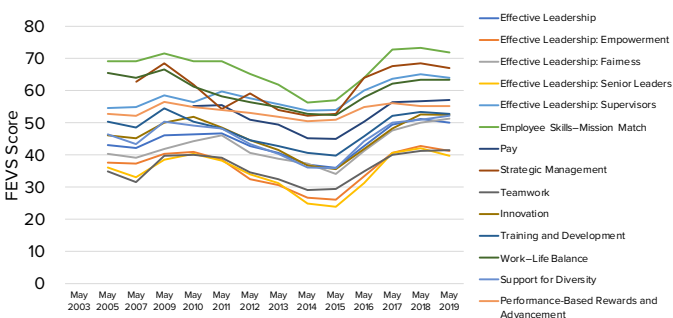
Source: Partnership for Public Service, *Best Places to Work in the Federal Government, 2019*

Figure 6: US Secret Service FEVS scores by category



Source: Partnership for Public Service, *Best Places to Work in the Federal Government, 2019*

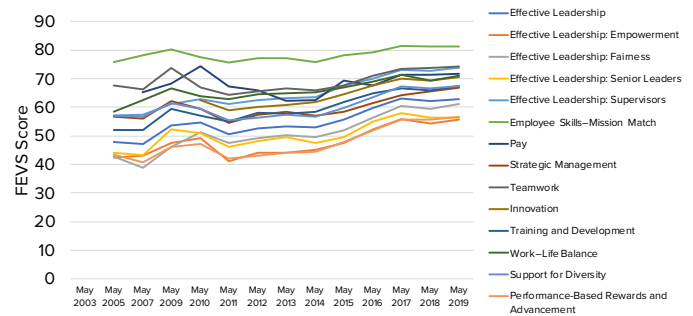
Figure 7: ICE FEVS scores by category



Source: Partnership for Public Service, *Best Places to Work in the Federal Government, 2019*

- **I&A under Under Secretary Frank Taylor, 2014-17:** Brig. Gen. Francis X. Taylor, USAF (ret.) took office as under secretary of I&A in early June 2014. He reorganized I&A to address a top-heavy management structure and poor performers who were preventing the promotion

Figure 8: US FEVS scores by category



Source: Partnership for Public Service, *Best Places to Work in the Federal Government, 2019*

of those who were more qualified. As is often the case during a reorganization, morale declined in the first year, but increased steadily for the next two years (Figure 5). In May–June 2017, I&A's FEVS scores across the board were higher than before Taylor took office.

- **USSS under DHS Secretary John F. Kelly and USSS Director Randolph “Tex” Alles:** USSS was rocked by scandal starting in 2012 when agents had to be disciplined for hiring prostitutes in Cartagena, Colombia. This revealed a number of problems within the USSS culture that took several years to address. The decline was halted in 2016 and 2017 under DHS Secretary Jeh Johnson, then morale improved steadily from 2017 to 2019 under Secretary John F. Kelly and Director Randolph “Tex” Alles, erasing most of the loss (Figure 6). Former DHS employees attributed the success to Secretary Kelly, a former Marine Corps general, who showed a strong, personal interest in the USSS officers he encountered at the White House, both as secretary and when he was chief of staff to the president, and to efforts by Director Alles to develop an employee engagement action plan, to address agents’ concerns about work-life balance, and to other actions.
- **ICE under Director Sarah Saldaña** underwent an even stronger surge in employee morale from 2015 to 2017 (Figure 7).
- **USCG and USCIS** have long been at the top of DHS’s components in FEVS surveys. While USCG might be thought of as unlike other DHS components because of its core of uniformed personnel, **USCIS is DHS’s other long-term morale success story.** USCIS had shown a steady, year-on-year improvement in almost all categories (Figure 8). USCIS has a history of being led by immigration law experts and practitioners. USCIS’s last three years of survey data, from 2017 to 2019, were the



Secretary of Homeland Security Jeh Johnson visits with Iraqi refugee Jaafar Ghassan Jaafar Abu-Ragheef and his family in New York City, June 10, 2016. *Source:* DHS photo by Barry Bahler

highest in USCIS's history and were the continuation of trends from previous years.

DHS morale can be turned around. Internal DHS success stories demonstrate this. Just as DoD turned around its morale issues after the Vietnam War ended in 1975, improving DHS's morale will likely take an effort of comparable scope and will need to be sustained over more than one presidential term. However, as DHS's success stories show, it may be possible to begin to see significant improvements in twelve to eighteen months.

Recommendations for Improving Morale at DHS

- 3.1 DHS's headquarters and component leaders need to recognize that morale at DHS can be improved by sustained focus and attention on the underlying workforce issues driving the department's low morale.**
- 3.2 DHS needs to move to a "culture of cultures" approach, celebrating the unique aspects of each component, while providing a unifying cultural overlay around a mission that most of its employees can embrace.** In the uniformed military, services and specialized units have strong individual cultures but the services share a common ethos and many common values. This may not be a perfect model for DHS, but it provides a validating example.
- 3.3 Public trust and support for DHS's mission is vitally important.** If the American people do not genuinely value what DHS is doing, the department will have trouble improving overall morale.⁸⁷

Listen to what DHS employees are saying:

3.4 DHS should considerably increase two-way communications with its employees. DHS leadership should listen more to what employees are saying. DHS should brief national and departmental strategies to all employees so they know how their work contributes to such strategies.

3.5 DHS should make better use of the FEVS surveys as a management tool, sharing the results more widely within the department and, where necessary, looking for "red flags" among the data for warning signs of changes that need to be made. Using the FEVS survey in this way will demonstrate management support for the importance of the views of DHS employees—which itself will enhance morale within the Department by showing that employees' views matter. The problems of the CWMD office, noted above, which ranked 420 out of 420 in the 2019 survey, is a positive example. Significant negative responses to the question "My organization's senior leaders maintain high standards of honesty and integrity" deserve immediate investigation by the DHS front office and the DHS inspector general, and the results need to be shared with the employees.

3.6 DHS should create a career path for entry-level personnel, especially from TSA, to get preference for hiring into other DHS jobs with better long-term career prospects. One of the greatest problems at several DHS components, TSA especially (see below), is the perception that options for career advancement are often limited or not well-advertised. This leads to higher turnover, increased costs to train new personnel, and lower overall effectiveness because experienced people leave the organization. DHS should allow DHS employees to transfer more easily between components and within components. In particular, meritorious service in entry-level positions should give employees a preference that increases a candidate's prospects for being hired elsewhere in DHS or should open up training opportunities that would increase a candidate's ability to be hired for a better career-track position. And those DHS employees who are tied to a particular location—because of family reasons, for example—should be given outright preferment and service credit for other DHS jobs in the same area. This would increase employee satisfaction and give DHS the benefit of retaining employees with strong ties in the community. DHS needs to find ways of creating career paths for its entry level employees so that meritorious DHS employees stay with DHS.



TSA officers conduct patrols at Union Station. Source: DHS photo by Barry Bahler

TSA

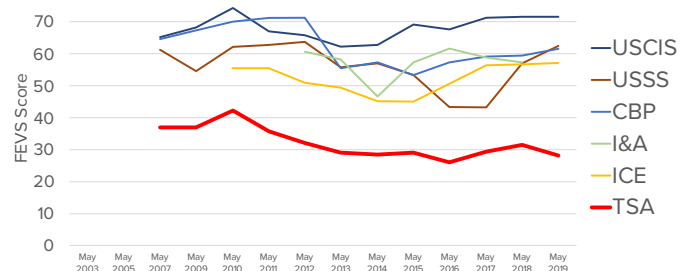
3.7 Morale at TSA can be improved by urgently addressing issues of pay, promotions and career advancement, and employee empowerment. FEVS data show clearly what it will take to improve morale at TSA. TSA has long had low overall morale—in 2019, for example, TSA was ranked 398 out of 420 subagencies. Apart from two much smaller components—I&A and CWMD—TSA was the lowest-ranked component of DHS.

TSA employees' low pay (Figure 9) is a problem that cries out for correction. TSA scores are half of those

at CBP, ICE, I&A, USCIS, and USSS. As one expert in this project's study group said, TSA is competing for talent against Amazon fulfillment centers—and losing.

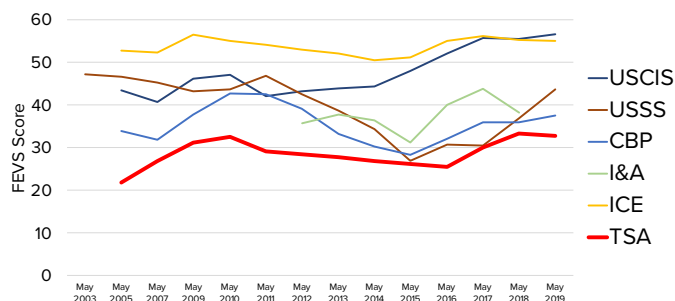
TSA has similar problems offering its employees, especially screeners, a career path with meaningful promotion and advancement (Figure 10). This is one reason so many screening officers leave TSA in the first three years compared to other positions in TSA and the federal workforce generally. The cost of turnover to TSA is high.⁸⁸ **Recommendation 3.4 above addresses this problem by calling on DHS to develop**

Figure 9: FEVS scores by component: Pay

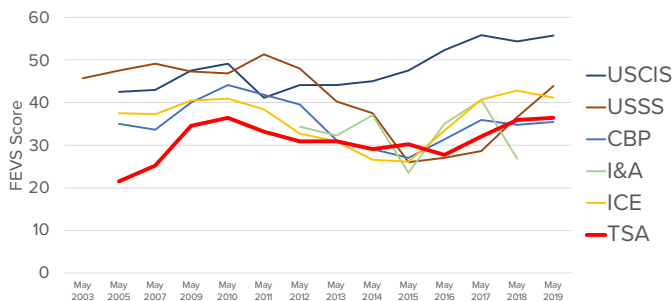


Source: Partnership for Public Service, *Best Places to Work in the Federal Government*, 2019

Figure 10: FEVS scores by Component: Performance-based rewards and advancement



Source: Partnership for Public Service, *Best Places to Work in the Federal Government*, 2019

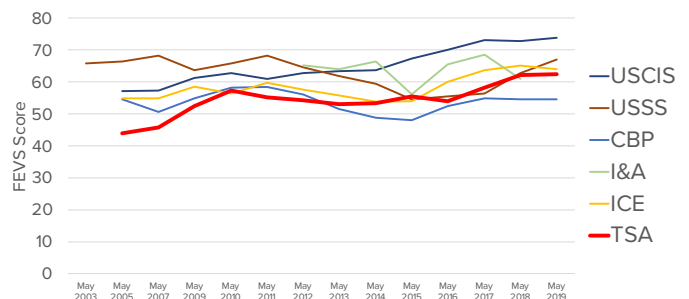
Figure 11: FEVS scores by component: Effective Leadership – EmpowermentSource: Partnership for Public Service, *Best Places to Work in the Federal Government*, 2019

career paths by giving meritorious TSA entry-level employees the increased ability to be hired for other positions at DHS with more career potential.

TSA has likewise never been out of the lower end of the range of DHS components on empowering its employees (Figure 11). TSA's procedures and work rules may have had to be strict in the early days right after 9/11—itself a failure of aviation security screening—but today the threat picture is different, and there were indications from study group participants that TSA's lack of employee empowerment contributes to excessive turnover. (The fact that other DHS components have fallen to TSA's levels shows that lack of empowerment is a problem in more of DHS than just TSA. In 2017-19, only 38.7 percent of DHS employees agreed they had “a feeling of personal empowerment with respect to work processes,” one of the lowest scores on this question in the federal civilian workforce. The government-wide average is 48.6 percent, almost 10 percentage points higher than DHS.)

As noted in the previous three paragraphs, TSA stands out negatively compared to other DHS components in low pay, lack of promotion, limited career opportunities, and lack of employee empowerment. Significantly, in other respects TSA does *not* stand out. Employees at DHS regard their immediate supervisors relatively highly, and TSA is no exception (Figure 12). The same can be said for TSA being in the middle of DHS component scores for matching employees to the mission, teamwork, and innovation. **It is only on low pay, lack of promotion, limited career opportunities, and lack of employee empowerment that TSA stands out.**

A separate group of experts convened by TSA Administrator David Pekoske⁸⁹ to look at TSA's human

Figure 12: FEVS scores by component: Effective Leadership – SupervisorsSource: Partnership for Public Service, *Best Places to Work in the Federal Government*, 2019

capital problems independently reached similar conclusions to those set out above. Their report, released by ICF Consulting in May 2019,⁹⁰ found deficiencies in the TSA Office of Human Capital. It cited the 2018 TSA Exit Survey saying departing TSA employees were concerned about leadership issues, including a lack of management skills, unfair practices in performance appraisals and career advancement, a hostile work environment, and inadequate communication with the TSA workforce. This study also concluded that pay for screeners “is a key issue for the screening workforce.” In particular, screeners were aggrieved that their pay was one-third of TSA employees in “Management, Administration and Professional” positions. The pay and performance management system was so flawed that a screener starting out in the lowest TSA pay band, the “E-band,” even with exceptional performance ratings every year, would take more than thirty years to rise to the top of the E-band.

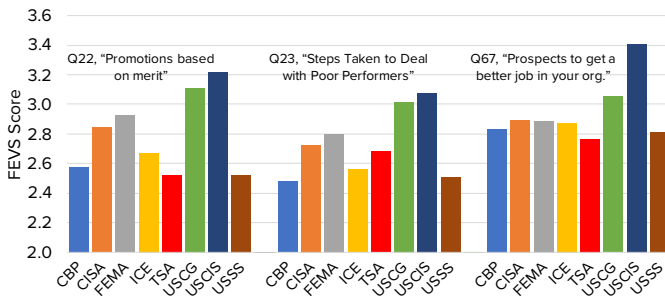
If TSA's morale can be raised by fifteen to eighteen points, that alone would be enough to raise DHS out of last place in federal workforce morale.

A fifteen to eighteen-point increase is comparable to what happened at I&A under Taylor in 2015-17, USSS under Alles in 2017-19, and ICE under Saldaña in 2015-17. **With money from Congress for better pay, by giving TSA employees the prospect for a meaningful career, and by empowering TSA's employees, TSA can help lead a turnaround in DHS morale.**

CBP

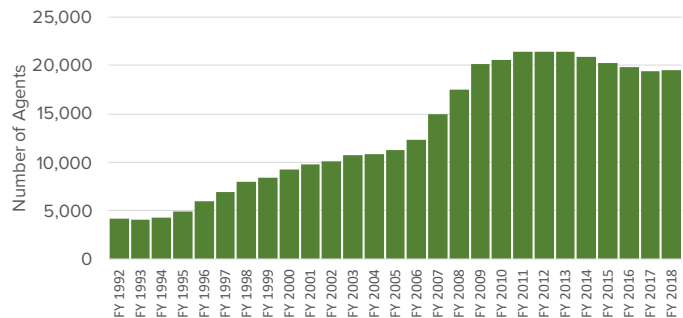
3.8 CBP presents a totally different picture—CBP needs to address problems relating to trust, how it deals with poor performers, and promotions. CBP is consistently among the lowest three DHS components

Figure 13: Response to FEVS Questions 22, 23, and 67 by DHS component, 2017-19 3-Year Average



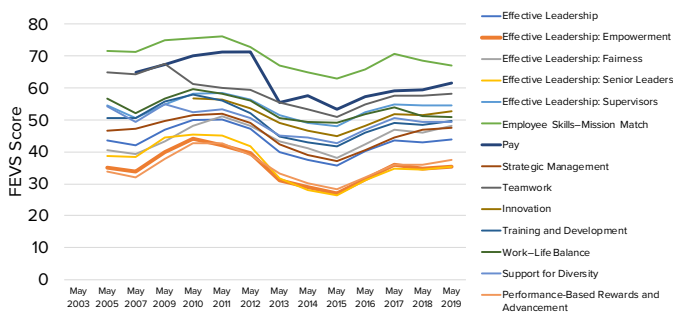
Source: Office of Personnel Management, FEVS, *Report by Agency*

Figure 15: US Border Patrol staffing by fiscal year



Source: CBP, <https://www.cbp.gov/sites/default/files/assets/documents/2019-Mar/Staffing%20FY1992-FY2018.pdf>

Figure 14: CBP FEVS scores by category



Source: Partnership for Public Service, *Best Places to Work in the Federal Government, 2019*

(Figure 13) on whether promotions are based on merit (FEVS question twenty-two). More importantly, CBP employees do not see that steps are taken to deal with poor performers (question twenty-three)—here again, CBP’s score is the lowest among major components. Nor are CBP employees particularly satisfied with their own prospects of getting a better job within CBP or DHS (question sixty-seven).

CBP also rates significantly below DHS averages on whether rewards and advancement are based on merit (Figure 10). CBP’s lowest FEVS scores, consistently, are employee empowerment, performance-based rewards and advancement, and how CBP employees rate senior leaders (Figure 14).

One of the most important events affecting CBP morale was the announcement between May 2012 and May 2013 of a change in how CBP paid officers for uncontrollable overtime.⁹¹ After a “stinging” report by the Office of Special Counsel on the abuse of admin-

istratively uncontrolled overtime (AUO), the National Border Patrol Council and Congress together agreed to eliminate AUO in return for higher base pay.⁹² Many CBP officers saw their total take-home pay drop by about \$6,500 a year because of the loss of paid overtime.⁹³ Morale at CBP had been good prior to 2013, but this change led to a drop (shown in Figure 14) from which CBP morale has not yet fully recovered. This negatively affected CBP employees’ views of their senior leaders, employee empowerment, and most other factors as well.

A second issue relates to the rapid expansion of the Border Patrol from FY 2006 through FY 2011 (Figure 15). One historian wrote, “CBP recruited that new army by lowering its hiring standards ... and shoveling agents through the academy and into the field before even completing background checks.”⁹⁴ Procedural changes to allow CBP to address corruption in its ranks have languished.⁹⁵ A March 2016 Homeland Security Advisory Council report concluded “The CBP discipline system is broken. The length of time from receiving an allegation of misconduct to imposing final discipline is far too long.”⁹⁶ Congress had failed to give CBP the authority to discipline its own ranks.⁹⁷ Investigations became turf battles among the DHS inspector general, FBI, ICE, and CBP’s internal affairs office.⁹⁸ When one of the two Senate-confirmed commissioners since February 2009, Gil Kerlikowske, brought in Mark Morgan to head the Border Patrol, one journalist noted “Morgan’s outsider status and the reform agenda had so angered the Border Patrol union that axing him was No. 1 on its wish list when Trump came into office....”⁹⁹ Morgan left CBP on January 26, 2017, and returned to CBP in July 2019, when he was named the senior official performing the duties of the CBP commissioner.



Border Patrol agents patrol on vehicles. *Source:* CBP photo by Ozzy Trevino

Another negative factor affecting CBP morale was the practice of releasing detained migrants into the community while awaiting immigration or asylum proceedings, known by the derogatory term “catch-and-release,” likening the migrants to sport fish who get caught only to be released back into the water to be caught again. To many in CBP, especially in the Border Patrol, this practice had the effect of negating their service to their country, since their best efforts to stop people from coming into the United States between official ports of entry were undone by practices they felt were set by judges or higher officials who did not value their work. DHS should devise a border and immigration management system that can get the support of Congress and the American people and does not devalue the Border Patrol’s work.

DHS and CBP should think about whether a change in Border Patrol culture would be beneficial for Border Patrol officers and for the Border Patrol itself. A journalist assessing the mid-2019 southwest border crisis wrote, “Most Border Patrol agents serving today signed up for a tough job in a quasi-military agency protecting the country against terrorists and drug dealers. They’ve found themselves instead serving as a more mundane humanitarian agency—the nation’s front-line greeter for families of migrants all too happy to surrender themselves after crossing the

border. CBP’s [sic] doesn’t have the culture to meet this challenge, nor does it have the manpower or support from the rest of government.”¹⁰⁰

While most people saw the 2019 border crisis in humanitarian or partisan terms, the crisis made CBP’s morale problems worse. CBP’s mid-2019 budget supplemental request asked for an additional \$2.1 million for the Employee Assistance Program “to offer additional counseling services to CBP officers and personnel....”¹⁰¹ An additional \$1.1 billion in emergency supplemental funding in July 2019¹⁰² helped CBP’s resource problems, but it did little to solve CBP’s other underlying problems.

The need for counseling programs for CBP personnel predated the 2019 border crisis. A news organization in 2019 uncovered the shocking statistic from a CBP document that CBP’s suicide rate for each year 2015-2018 was 38 to 40 percent higher than the national average law enforcement suicide rate (16.66-16.90 per 100,000 officers vs. 12 per 100,000 officers).¹⁰³ A 2010 CBS News report documented similar strains on CBP officers.¹⁰⁴ In September 2015, CBP senior leaders publicly observed Suicide Prevention Month with a program “It’s OK to Call” to the Employee Assistance Program.¹⁰⁵ In 2019, DHS’s Chief Human Capital Office was working across all DHS components to



CBP Global Entry kiosks. *Source:* DHS/CBP photo by James Tourtellotte

try to prevent suicides.¹⁰⁶ While extreme, this shows a human facet of the importance and urgency of prioritizing improving morale at CBP.

CBP needs Senate-confirmed leadership empowered by DHS’s headquarters to take the following actions to deal with urgent workplace issues that are driving low morale at CBP:

- a. Establish a discipline system that can move quickly, but fairly, to deal with poor performers, especially those who show susceptibility to corruption.
- b. Ensure a fair promotion process.
- c. Increase two-way communications and trust between CBP employees and CBP’s headquarters, and between CBP and the communities in which it works.

Additional recommendations

3.9 DHS needs to devote more resources to training incoming personnel about what the different parts of DHS do. Entry-level employees need a revamped and improved “DHS 101” course—so that all employ-

ees understand the culture of other large DHS components and what they do, and how the components and headquarters work with each other. This also needs to be part of long-term career path development. This should be reinforced with a “DHS 201” course for newly promoted supervisors, and a “DHS 301” course for middle management. A “DHS 401” course comparable to the DoD Capstone program should be developed to train DHS members of the Senior Executive Service. **DHS also needs a separate program with employee engagement to develop the “culture of cultures” idea in ways that build both cohesion within components and cohesion across components.**

3.10 DHS needs to supplement the FEVS annual surveys with resources for headquarters and components to conduct “pulse” surveys (fewer questions, but more frequently) to better understand factors driving employee morale. FEVS has several limitations—it is administered annually, asks the same questions, and is ambiguous as to whether “senior leaders” refers to department or component leadership. DHS should commission additional surveys and focus groups to assess progress on morale initiatives.

IV. Fixing the Internal Challenges That Hold DHS Back

Key Findings

Fixing DHS's morale problems should be one of the department's top management priorities, but there are other priorities that are not far behind.

While DHS is often referred to as a department consolidated out of twenty-two separate federal agencies or programs, the reality is different. **As enacted by Congress and through subsequent legislation and appropriations practice, the Homeland Security Act created a weak and under-resourced DHS headquarters and relatively autonomous "components"** where most of DHS's 240,000 employees work and where most of DHS's annual budget of \$62 billion is spent. DHS is sometimes thought of as medieval France, where a series of powerful feudal barons pay only nominal allegiance to a high king or queen.

DHS will never achieve its potential as a cabinet department until it addresses its headquarters-component problems and achieves a greater unity of effort, which has been a goal of every secretary of homeland security. Interviews with former DHS officials and the experts who contributed to the Future of DHS study groups all point to the headquarters-component divide as being one of the keys to DHS's perceived dysfunction. While this problem exists to some degree at many large, dispersed organizations, many who worked at DHS or in other large government or private organizations all acknowledged that DHS has it far worse. Many former DHS employees saw themselves in one or both of these two descriptions:

- Component personnel think headquarters does not understand component operational practicalities.
- Headquarters personnel think components do not see the big picture or appreciate that external factors sometimes require changes in what components do and, in some cases, how they do them.

There is substantial truth in both viewpoints. DHS needs to close the gap between these perceptions.

DHS should better coordinate policy and resources. Headquarters has an important role, beyond just the secretary and deputy secretary, in coordinating both policy and resource decisions across the department. Effective constitutional governance requires that policy priorities should be translated into budgets and operations. DoD has

mechanisms to ensure DoD operations are aligned with national policy. DHS, on the other hand, does not.

At DHS, policy changes come either from within DHS or from the top down—from the White House, from Congress, and from outside events. Budgets at DHS are built bottom-up, because DHS's components are where the people, capabilities, and technology are, and where all of the front-line DHS missions are carried out.

Instead of aligning to national priorities and strategies, DHS's budget processes align to the operational requirements of DHS's components.¹⁰⁷ While this leads to incremental improvements based on ground-up input from operators, former officials noted that this sometimes fails to take into account external shocks and developments outside of what component leaders anticipate based on day-to-day operations. The disconnect between policy and resources makes it harder for DHS and its stakeholders to get support for important initiatives from the White House's Office of Management and Budget and from Congress.

DHS headquarters, according to former DHS officials, is not always seen by components as authoritative or final in budget matters. The DHS budget process contributes to the president's budget submission to Congress, usually in February of each year. This is followed by a separate process in which component leaders interact directly with the congressional committees or subcommittees. This often leads to adjustments that experts believe have proven literal lifesavers to key DHS missions—including by DHS's own admission. In 2017, the Trump administration said it was closing the DHS Science and Technology Directorate (S&T) National Biodefense Analysis and Countermeasures Center (NBACC) to save money.¹⁰⁸ The proposed cuts were restored by Congress.¹⁰⁹ DHS acknowledged in early 2020 that NBACC was "initiating crucial research to mitigate COVID-19."¹¹⁰

Currently, the chains of authority for DHS policy and resource decisions are not unified until they rise to the level of the secretary or deputy secretary, and lateral communications channels are weak or nonexistent. In the view of many former DHS officials, component senior leaders do not take policy initiatives seriously unless they come from the secretary or deputy secretary. Former DHS officials believe it often takes the secretary or deputy secretary of homeland security to take a sustained, personal interest in



CBP's autonomous surveillance towers. Source: U.S. Customs and Border Protection

a specific issue to drive change over the objections of the senior working-level officials (GS-15) in DHS's components.

Shifting resources and sometimes personnel to meet urgent, unbudgeted needs is one of DHS's greatest—and most recurring—challenges. Historical examples include Hurricane Katrina (2005), the terrorist liquids plot (2006), the underwear bomb plot (2009), the laser printer toner cartridge plot (2010), the rise of ISIS and the Khorasan Group (2014), the border crisis of 2014, the border and immigration crisis of 2019, and most recently COVID-19 (2020). Some of these events drove major policy changes, others drove significant resource changes, and some drove both.

Some resource shifts can be in the billions of dollars, but sometimes rapid shifts of a few million dollars or a few hundred personnel assigned to a project in advance of a threat can result in improved security for the homeland and the American people.

History shows these problems are often the result not of failures at DHS, but failures of the executive branch or Congress to adequately budget for needs that may have been—and often are—foreseen by DHS professionals. This

problem runs deep. This challenge has gotten more difficult in recent years, and many outside experts in homeland security agree the challenge will get more difficult in the future if DHS does not put effort into making policy and resources align, and to being able to reallocate resources and priorities in a crisis.

DHS would benefit from changing the way it staffs headquarters, so that approximately half of key headquarters offices are component personnel on “joint duty” assignments, and the rest are a cadre of permanent headquarters personnel. DHS needs to build stronger bonds of understanding and mutual support between headquarters and components by a “jointness” approach under which half of all major headquarters units such as PLCY and Management Directorate (MGMT) personnel would be detailees from the components. DoD's comparable program, mandated by the 1986 Goldwater-Nichols Act, proved one of the most effective steps DoD ever took to build “jointness” in the US military, according to numerous military and civilian leaders at DoD.

DHS should considerably enhance two-way communications between headquarters and components. At the heart of the issues between DHS headquarters and

components is a communications challenge. Information does not flow smoothly or easily, a problem made more challenging by geographical dispersal both of components from headquarters and from field offices around the country.

A further problem is the “parallel universes” in which DHS personnel work. Many employees use only unclassified, official-use-only computer systems, and still others work almost entirely on mobile devices. Others work in highly classified facilities, and still others work on the Secret-level systems of the national security policy community. DHS needs solutions that bridge these different data and communications systems and approaches, while being able to protect both personal privacy and classified information.

A further challenge is coming in the need not just to communicate, but to communicate more quickly—at network speeds—between operational units and between headquarters and components. **DHS needs additional personnel and resources to speed up and enhance communications within DHS.**

Recommendations for Fixing DHS’s Internal Problems

4.1 Policy and budget officials at DHS’s headquarters should work much more closely together and have frequent, secure communications since most national security policies and strategies are classified. **DHS needs to significantly increase the resources dedicated to policy-resource coordination at DHS headquarters**—especially between PLCY and MGMT below the under secretary level, but also including the chief financial officer (CFO) and between DHS headquarters at St. Elizabeths and the DHS financial personnel at 7th and D Street. Additional personnel—probably ten or twenty, but not hundreds—need to be assigned to making sure the necessary information on policy flows to budget formation, and that financial information flows back to policy officials. Senior policy and management officials at the GS-15 and SES levels need to devote more time to understanding what each other is doing and why. This may require additional higher-level security clearances for MGMT and budget personnel when the reasons for resource allocations requires knowledge of classified reasons behind policy decisions.

Because strategies are often classified while budget decisions are not, DHS needs to develop a secure alerting mechanism so that those who work in classified spaces and those who work in unclassified spaces can both communicate critical updates and relevant policy changes. Policy decisions and

budget decisions sometimes move slowly, but both go through periods where war and peace—and the resources to fight a war or win a peace—need to be decided in minutes with each informing the other. DoD has systems and procedures in place. DHS does not. To help with this, DHS could standardize on a common platform for secure communications—bringing together devices, applications, and mobile communications, including protecting DHS’s mission-enabled applications.

Expecting the unexpected needs to be a normal, permanent part of how DHS coordinates policy and resources. DHS needs to be able to adjust money and people quickly and easily because DHS will always face urgent threats and issues—such as the rise of the next ISIS, or a series of natural disasters that overwhelm state and local governments, or a massive state-sponsored cyberattack—that were not foreseen as part of the budget or long-term policy development process.

4.2 PLCY needs to devote considerably greater efforts to better communication throughout DHS operational components of national and DHS policy priorities. This includes changes in policy, the context surrounding those changes, and possible future directions for policy changes.¹¹¹ DHS should standardize on a common platform to effectively and swiftly communicate policy updates to all relevant personnel. As much as possible, component leadership should never be surprised by changes in policy. This will require additional headquarters and component personnel to ensure information is disseminated laterally and vertically, especially within components. It will also require DHS to invest in classified connectivity because most national security policies and strategies are classified. This will also require policy officials and chiefs of staff at headquarters and components to communicate the results of their work to more people.

4.3 DHS needs to set up a department-wide personnel rotation policy to bring headquarters and components closer together. Components need to rotate personnel—including some of their best people—in tours at headquarters so that they gain headquarters experience.

Just as military promotions beyond a certain level now require joint duty, successfully serving a tour at DHS headquarters should be rewarded in promotion decisions in components—and required for promotions to GS-15 or higher. Tours should be for two to three years, with the possibility of a one-year

extension. DHS headquarters units—including PLCY, MGMT, I&A, OPS, OLA, OPA, OIG, OPE, PRIV, CRCL—should set up positions for such detailees such that half of all personnel in those offices would eventually be component detailees, and half would be permanent headquarters personnel. The overall DHS budget would be largely unchanged, and whether detailees should remain on the payroll of their permanent component or transferred to the payroll of the receiving component is not that important—but DHS needs to ensure that detailees receive bonuses and awards from the component where they are working, and appropriate recognition when they return home.

DHS headquarters needs to start requiring GS-13 personnel and below to serve in a component for at least two years in order to be promoted to GS-15 or SES. Components would advertise open positions so that headquarters personnel could apply for them and receive training if needed.

DHS personnel from components and headquarters should also establish rotational slots to congressional staff positions and to other departments and agencies that are DHS’s key partners, such as the State Department’s Counterterrorism bureau and International Security and Nonproliferation bureau. (USCG and CBP already do this regularly; DHS headquarters and other components, less so.) Those personnel should first do a six- to twelve-month rotation to headquarters to develop a strategic view of departmental priorities before sending them to the Hill or another cabinet department.

4.4 DHS should make no major reorganizational changes in the next year, because the resulting disruption would take focus away from DHS’s more urgent mission and management challenges. DHS’s leadership should resist the efforts, which will come from well-meaning outside voices, to try to solve DHS’s problems by ordering a major reorganization of the department. DHS’s most urgent problems are re-focusing its mission, its approach to public-private partnerships, and the workforce issues that drive DHS’s morale. Moving DHS’s “boxes” around on an organization chart is not the best solution to these problems.

A number of ideas have been put forward to reorganize DHS. This ranges from broad-brush ideas to “Abolish DHS” or “Abolish ICE” to focused ideas like the June 2018 idea put forward by ICE Homeland Security Investigations (HSI) senior special agents to separate HSI from ICE’s Enforcement Removal Operations (ERO).¹¹² It also includes the Trump adminis-

tration proposal to move the US Secret Service from DHS to Treasury.¹¹³ The USSS proposal was motivated in part by concerns that USSS was not getting enough of the right kind of support from DHS headquarters and for a desire to be separated budgetarily from the ERO border enforcement mission.¹¹⁴

Any reorganization is time-consuming and causes disruption in the units affected by it, especially headquarters units. **Given the urgent threats from COVID-19, foreign nation-state non-military threats, the need to strengthen trust between DHS and the American people, and the management challenges discussed above, the experts involved in the Future of DHS Project strongly recommend DHS focus on its core problems and not move boxes around organizationally in the next year.** There are, however, two smaller changes that would have an immediate, beneficial effect.

4.5 DHS should have an “S3” deputy secretary-level official just below the current deputy secretary in rank to coordinate DHS’s law enforcement components. Given the breadth of DHS missions, both the secretary of homeland security (known as “S1” inside DHS) and the deputy secretary (“S2”) have broader responsibilities than their counterparts at other cabinet departments. DHS should have an “S3” deputy secretary-level official, just below the current deputy secretary position, to give DHS senior leadership more capacity to cover the full range of DHS’s issues. (To keep titles straight, S2 could become the “principal deputy secretary.”) Another recent expert study of DHS’s management structure independently reached this same conclusion.¹¹⁵

The most pressing need for a third top DHS official is to coordinate DHS’s law enforcement components—some or all of ICE, CBP, the Federal Protective Service, and USSS. DHS has more law enforcement personnel than any other government department, including DOJ. As noted above, DHS’s law enforcement components have significant internal challenges of trust, morale, organization, and accountability, as discussed above in connection with CBP (see Recommendation 3.8) and the tension within ICE between HSI and ERO (see Recommendation 4.4). DHS will need to look at the role of legal authorities of DHS’s different law enforcement arms in light of criticisms DHS received in the summer of 2020. The underlying reasons offered for transferring USSS to Treasury—that USSS is not getting the attention and resources it needs from the DHS front office—need to be addressed by DHS headquarters even if USSS stays in DHS, as the Future of DHS Project’s experts recommend.

The most appropriate solution here is to look at the model of DOJ, which has a deputy attorney general who acts as the primary backup to the attorney general and who oversees parts of DOJ, and an associate attorney general, who oversees the Civil Division and other offices, and is DOJ's third-ranking official.¹¹⁶

An "S3" deputy secretary-level official, just below the current deputy secretary in rank, would be able to coordinate the law enforcement components of DHS. If DHS's deputy secretary ("S2") has a law enforcement background, that person could serve such a role—but then "S3" would be necessary to free up some of the deputy secretary's time to handle the law enforcement coordination responsibility.

A second deputy secretary as "S3" would be a better solution than moving all of DHS's law enforcement functions under a single under secretary, who would have full control over DHS law enforcement. **DHS headquarters should not politicize law enforcement within DHS.** The staff of a second deputy secretary, like the staff of the current DHS deputy secretary—which includes a chief of staff and several advisers and assistants—should be sufficient so that DHS's law enforcement components have the right degree of policy oversight and accountability without micro-management.¹¹⁷

DHS would need to request authorization from Congress for this change, but until Congress acts, DHS should empower a very senior DHS official to coordinate DHS's law enforcement agencies by a designation and a delegation of authority from the secretary. There is precedent for this in the way former DHS Secretary Janet Napolitano began the tradition—continued by subsequent secretaries—of designating a DHS under secretary (the next-highest rank at DHS below the deputy secretary) to serve as the DHS counterterrorism coordinator to coordinate

and provide oversight over DHS's counterterrorism policies and operations.

4.6 DHS should return policy officials working biological, chemical, and nuclear threat issues to PLCY. In 2017, DHS set up the Countering Weapons of Mass Destruction office (CWMD), headed by an assistant secretary.¹¹⁸ This included "certain personnel from PLCY and the Office of Operations Coordination with expertise on chemical, biological, radiological, and nuclear issues."¹¹⁹ Congress passed the Countering Weapons of Mass Destruction Act in December 2018, but gave CWMD policy responsibility only for terrorists' use of CWMD, not for pandemic disease.¹²⁰ Moving policy experts to the CWMD component diminished their influence, because they were focused on CWMD's low-risk, high-consequence mission of countering *terrorists'* use of WMD, not on the more likely and equally high-consequence mission of addressing pandemic disease.¹²¹

While DHS components are organized operationally, PLCY is organized around policy issues, like counterterrorism, trade, immigration, or cybersecurity, for example; or around policy-informing stakeholders, such as international affairs. Sending PLCY's biohazard experts to CWMD as part of the 2017 reorganization meant they would focus on terrorist use of WMD, not all-hazard biological threats that include *both* terrorism and pandemic disease. Given DHS's immediate need in 2020 and 2021 to focus on policy issues relating to the immediate threat of COVID-19, in addition to any threats from terrorist groups, those CWMD policy officials, and the responsibility for developing related policies, should be returned on a permanent basis to PLCY to support the DHS under secretary for policy and other policy officials who deal with threat prevention. **Addressing the challenge of COVID-19 needs to be DHS's top short-term priority until COVID-19 is no longer the threat it is today.**

Conclusion

The forward defense of the United States faces different challenges from those that US leaders faced in 1945, 1989, or even in 2016. A strong military, backed by a strong economy, a vibrant democracy, and US diplomacy, are all vitally necessary but are no longer sufficient.

The US Department of Homeland Security was created in 2003 to help ensure the United States never again experienced an attack like 9/11. Underlying that decision was the recognition that in 2001, the world had changed to the point where nonmilitary means—four passenger aircraft—could be used to kill more Americans than died in

the attack on Pearl Harbor in 1941. It should focus US policymakers that, as of August 2020, the COVID-19 pandemic is killing as many Americans as died on 9/11—**every four days**. The COVID-19 pandemic, the increasing non-kinetic actions by nation-state adversaries that seek to undermine American power, and the long-term threat to US infrastructure from climate and weather changes, all point to the need for the United States to make another fundamental change in how the US government defends the nation and keeps the American people safe. The best solution available is to refocus the Department of Homeland Security and to fix DHS's internal problems so it can lead the defense of the nation against nonmilitary threats.



The American flag, DHS flag, and Border Patrol flag in McAllen, Texas. Source: DHS photo by Barry Bahler

Annex 1:

Glossary of Abbreviations, Acronyms, and Initialisms Used in This Report

CBP	Customs and Border Protection, a DHS component, headed by the commissioner. Constituent units include the Office of Field Operations, the Border Patrol, and Air & Marine.		
CISA	Cybersecurity and Infrastructure Security Agency, a DHS component, headed by a director. Formerly known as the National Protection and Programs Directorate in DHS headquarters, headed by an under secretary.		Includes the DHS chief financial officer (CFO), chief procurement officer, chief human capital officer (CHCO), chief readiness support officer, chief security officer (CSO), and chief information officer (CIO), and the respective offices that carry out those functions. Also includes the Office of Biometric Identify Management, and, since May 2019, the Federal Protective Service.
CRCL	Office of Civil Rights and Civil Liberties, headed by the officer for civil rights and civil liberties. Reports directly to the secretary.	NBACC	National Biodefense Analysis and Countermeasures Center, a unit within DHS S&T.
CWMD	Countering Weapons of Mass Destruction Office, established in 2017, headed by an assistant secretary.	OGC	Office of the General Counsel, reports to the secretary, headed by the general counsel.
DHS	Department of Homeland Security, headed by the secretary of homeland security and a deputy secretary of homeland security.	OIG	Office of the Inspector General, nominally reports to the secretary, headed by the inspector general.
FEMA	Federal Emergency Management Agency, a DHS component, headed by an administrator.	OLA	Office of Legislative Affairs, reports to the secretary, headed by an assistant secretary.
FLETC	Federal Law Enforcement Training Center, a part of DHS that reports directly to the secretary, headed by a director.	OPA	Office of Public Affairs, reports to the secretary, headed by an assistant secretary.
I&A	Office of Intelligence & Analysis, headed by an under secretary. I&A is a part of the US Intelligence Community and listed in Executive Order 12333. Most operational components also have their own intelligence offices to support component decisionmaking and operations.	OPE	Office of Partnership & Engagement, an office that reports directly to the secretary that coordinates engagement with DHS state, local, tribal, and territorial governments, and the private sector, headed by an assistant secretary.
ICE	Immigration and Customs Enforcement, a DHS component, headed by a director (formerly titled assistant secretary). Constituent units include Homeland Security Investigations (HSI) and Enforcement and Removal Operations (ERO).	OPS	Office of Operations Coordination, an office that reports directly to the secretary, headed by a director.
MGMT	Management Directorate, a unit of DHS headquarters, headed by an under secretary.	OSEM	Office of the DHS Secretary and Executive Management, effectively the budget-line item that covers the DHS front office, including the secretary and deputy secretary, as well as MGMT, PLCY, and other headquarters components and offices.
		PLCY	Office of Strategy, Policy, and Plans, a component within DHS headquarters, headed by an under secretary.

Future of DHS Project: Key Findings and Recommendations

PRIV	Privacy Office, headed by the chief privacy officer. Reports directly to the secretary.	TSA	Transportation Security Administration, a DHS component, headed by an administrator.
S&T	Science and Technology Directorate, which reports to the secretary, headed by an under secretary.	USCG	US Coast Guard, a DHS component, headed by the commandant.
SLTT	State, local, tribal, and territorial governments. Sometimes refers to law enforcement within those jurisdictions.	USCIS	US Citizenship and Immigration Services, a DHS component, headed by a director.
		USSS	US Secret Service, a DHS component, headed by a director.

(Note: DHS titles for component heads reflect DHS's historical roots. Use of the definite article "the" in front of a title indicates DHS has only one official with that title (e.g., "the commissioner [of CBP]" or "the general counsel." Use of "a" or "an" refers to a title used more than once (e.g., the senior official in FEMA and TSA are both titled "administrator").

Endnotes

- 1 Thomas H. Armstrong, *Decision, Matter of: Department of Homeland Security—Legality of Service of Acting Secretary of Homeland Security and Service of Senior Official Performing the Duties of Deputy Secretary of Homeland Security*, Government Accountability Office, August 14, 2020, <https://www.gao.gov/assets/710/708830.pdf>.
- 2 Chad Mizelle, letter to Thomas H. Armstrong, August 17, 2020, https://www.dhs.gov/sites/default/files/publications/20_0817_ogc_gao-as1-succession-response.pdf.
- 3 Thomas H. Armstrong, *Decision, Matter of: Department of Homeland Security—Legality of Service of Acting Secretary of Homeland Security and Service of Senior Official Performing the Duties of Deputy Secretary of Homeland Security—Reconsideration*, Government Accountability Office, August 21, 2020, <https://www.gao.gov/assets/710/708944.pdf>.
- 4 Homeland Security Act, 6 U.S.C. § 101(b)(1)(A).
- 5 US Department of Homeland Security, “Leadership,” retrieved July 31, 2020, <https://www.dhs.gov/leadership>.
- 6 Partnership for Public Service, “Best Places to Work Agency Rankings,” retrieved July 19, 2020, <https://bestplacestowork.org/rankings/overall/large>.
- 7 US Department of Homeland Security, “About DHS,” retrieved July 19, 2020, <https://www.dhs.gov/about-dhs>.
- 8 Congressional Research Service, *Trends in the Timing and Size of DHS Appropriations: In Brief*, December 6, 2019, <https://fas.org/sgp/crs/homesecc/R44604.pdf>.
- 9 Cecelia Smith-Schoenwalder, “Coronavirus Model Decreases Death Projection as Mask Wearing Increases,” *U.S. News & World Report*, July 22, 2020, <https://www.usnews.com/news/health-news/articles/2020-07-22/coronavirus-model-decreases-death-projection-as-mask-wearing-increases> (77,000 additional deaths by November 1, 2020). The 9/11 death toll has been calculated to be 2,981. Thomas H. Kean and Lee H. Hamilton, *The 9/11 Commission Report*, National Commission on Terrorist Attacks Upon the United States, 2004, <https://www.9-11commission.gov/report/911Report.pdf>.
- 10 Johns Hopkins University of Medicine, *COVID-19 in the USA*, retrieved July 31, 2020, <https://coronavirus.jhu.edu>.
- 11 Olivia B. Waxman and Chris Wilson, “How the Coronavirus Death Toll Compares to Other Deadly Events From American History,” *Time*, April 6, 2020, updated June 28, 2020, <https://time.com/5815367/coronavirus-deaths-comparison/>.
- 12 Waxman and Wilson, “How the Coronavirus Death Toll Compares,” 2020.
- 13 Paul Krugman, “America Drank Away Its Children’s Future,” *New York Times*, July 13, 2020, <https://www.nytimes.com/2020/07/13/opinion/coronavirus-schools-bars.html>.
- 14 James Glanz and Campbell Robertson, “Lockdown Delays Cost at Least 36,000 Lives, Data Show,” *New York Times*, May, 20, 2020, <https://www.nytimes.com/2020/05/20/us/coronavirus-distancing-deaths.html>; Bill Chappell, “U.S. Could Have Saved 36,000 Lives If Social Distancing Started 1 Week Earlier: Study,” NPR, May 21, 2020, <https://www.npr.org/sections/coronavirus-live-updates/2020/05/21/860077940/u-s-could-have-saved-36-000-lives-if-social-distancing-started-1-week-earlier-st>.
- 15 Dan Diamond and Nahal Toosi, “Trump Team Failed to Follow NSC’s Pandemic Playbook,” *Politico*, March 25, 2020, <https://www.politico.com/news/2020/03/25/trump-coronavirus-national-security-council-149285>.
- 16 US Homeland Security Council, *National Strategy for Pandemic Influenza Implementation Plan*, May 2006, <https://www.cdc.gov/flu/pandemic-resources/pdf/pandemic-influenza-implementation.pdf>.
- 17 Executive Office of the President, *Playbook for Early Response to High-Consequence Emerging Infectious Disease Threats Biological Incidents*, 2016, <https://assets.documentcloud.org/documents/6819703/WH-Pandemic-Playbook.pdf>.
- 18 Emma Reynolds, Luke McGee, and James Frater, “One Graphic Explains Why Americans are Facing an EU Travel Ban,” *CNN*, June 30, 2020, <https://www.cnn.com/2020/06/30/europe/european-union-travel-us-graphic-intl/index.html>.
- 19 Robert Roos, “Homeland Security law leaves HHS in control of bioterrorism preparedness,” *Center for Infectious Disease Research and Policy*, November 22, 2002, <https://www.cidrap.umn.edu/news-perspective/2002/11/homeland-security-law-leaves-hhs-control-bioterrorism-preparedness>.
- 20 DHS, *National Response Framework, Fourth Edition*, October 28, 2019, https://www.fema.gov/media-library-data/1582825590194-2f000855d442fc3c9f18547d1468990d/NRF_FINALApproved_508_2011028v1040.pdf.
- 21 Max Brooks, “War Stories from the Future: Launch of New Forward Defense Practice,” *Atlantic Council*, June 18, 2020, <https://www.atlanticcouncil.org/commentary/event-recap/war-stories-from-the-future-launch-of-new-forward-defense-practice/>.
- 22 Robert S. Mueller III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* Volume I, Department of Justice, March 2019, <https://www.justice.gov/storage/report.pdf>.
- 23 Reports to this effect are too numerous to mention here, but among the best are:
 Jamie Fly, Laura Rosenberger, and David Salvo, *Policy Blueprint for Countering Authoritarian Interference in Democracies*, Alliance for Securing Democracy, German Marshall Fund of the United States, 2018, <https://www.gmfus.org/publications/asd-policy-blueprint-countering-authoritarian-interference-democracies>.
 Suzanne Spaulding, Devi Nair, and Arthur Nelson, *Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System*,

Future of DHS Project: Key Findings and Recommendations

- Center for Strategic and International Studies, May 2019, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190430_RussiaUSJusticeSystem_v3_WEB_FULL.pdf.
- Ross Babbage, *Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail*, Vol. I, Center for Strategic and Budgetary Assessments, 2019, https://csbaonline.org/uploads/documents/Winning_Without_Fighting_Final.pdf.
- 24 Isaac R. Porche III, *Fighting and Winning the Undeclared Cyber War*, RAND Corporation, June 24, 2019, <https://www.rand.org/blog/2019/06/fighting-and-winning-the-undeclared-cyber-war.html>.
- 25 Nicole Perlroth and Katie Benner, "Iranians Accused in Cyberattacks, Including One That Hobbled Atlanta," *New York Times*, November 28, 2018, <https://www.nytimes.com/2018/11/28/us/politics/atlanta-cyberattack-iran.html>.
- 26 Testimony of FBI Director Christopher Wray before the Senate Judiciary Committee, July 23, 2019, as reported in Doina Chiacu, "FBI Director Wray: Russia Intent on Interfering with U.S. elections," Reuters, July 23, 2019, <https://www.reuters.com/article/us-usa-election-security/fbi-director-wray-russia-intent-on-interfering-with-u-s-elections-idUSKCN1U1XW>.
- 27 Michael Schmitt, *U.S. Cyber Command, Russia and Critical Infrastructure: What Norms and Laws Apply?*, Just Security, June 18, 2019, <https://www.justsecurity.org/64614/u-s-cyber-command-russia-and-critical-infrastructure-what-norms-and-laws-apply/>.
- 28 Alina Polyakova and Daniel Fried, *Democratic Defense Against Disinformation 2.0*, Atlantic Council, June 2019, <https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation-2-0/>.
- 29 Suzanne Spaulding, Devi Nair, and Arthur Nelson, *Beyond the Ballot: How the Kremlin Works to Undermine the U.S. Justice System*, Center for Strategic and International Studies, May 2019, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190430_RussiaUSJusticeSystem_v3_WEB_FULL.pdf.
- 30 Emerson T. Brooking and Suzanne Kianpour, *Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century*, Atlantic Council, February 2020, 2, <https://www.atlanticcouncil.org/wp-content/uploads/2020/02/IRAN-DIGITAL.pdf#page=6>. Other reports to similar effect include *Suspected Iranian Influence Operation: Leveraging Inauthentic News Sites and Social Media Aimed at U.S., U.K., Other Audiences*, FireEye, August 21, 2018, <https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-FireEye-Iranian-IO.pdf>.
- 31 Ross Babbage, *Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail*, Vol. I, Center for Strategic and Budgetary Assessments, 2019, https://csbaonline.org/uploads/documents/Winning_Without_Fighting_Final.pdf.
- 32 Mary Clare Jalonick, "Democrats: Trump Must Tell Voters About Election Threats," Associated Press, July 23, 2020, <https://apnews.com/37638ce4b00eb4dc69b9a994573fffd8>.
- 33 Nancy Pelosi, *Pelosi, Schumer, Schiff, Warner Joint Statement Following ODNI Announcement Regarding Election Security and Foreign Threats*, July 24, 2020, <https://www.speaker.gov/newsroom/72420-1>.
- 34 Matt Viser, "Joe Biden, citing intelligence briefings, warns that Russia, China are engaged in election interference," *Washington Post*, July 17, 2020, https://www.washingtonpost.com/politics/joe-biden-citing-intelligence-briefings-warns-that-russia-china-are-engaged-in-election-meddling/2020/07/17/3ce81580-c89a-11ea-a99f-3bbdbf1af38_story.html.
- 35 William Evanina, *Statement by NCSC Director William Evanina: Election Threat Update for the American Public*, Office of the Director of National Intelligence, ODNI News Release No. 29-20, August 7, 2020, <https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public>.
- 36 Michael Chertoff, "The Hijacking of Homeland Security," *New York Times*, July 28, 2020, <https://www.nytimes.com/2020/07/28/opinion/homeland-security-portland-trump.html>.
- 37 *What economic goals does the Federal Reserve seek to achieve through its monetary policy?*, Federal Reserve Board, August 19, 2016, <https://www.federalreserve.gov/faqs/what-economic-goals-does-federal-reserve-seek-to-achieve-through-monetary-policy.htm>.
- 38 Thomas H. Kean and Lee H. Hamilton, *The 9/11 Commission Report*, National Commission on Terrorist Attacks upon the United States, 2004, <https://www.9-11commission.gov/report/911Report.pdf>.
- 39 "Press Briefing by Senior Administration Officials on the Killing of Osama Bin Laden," The White House, May 2, 2011, <https://obamawhitehouse.archives.gov/the-press-office/2011/05/02/press-briefing-senior-administration-officials-killing-osama-bin-laden>.
- 40 "Islamic State Group Defeated as Final Territory Lost, US-Backed Forces Say," BBC News, March 23, 2019. <https://www.bbc.com/news/world-middle-east-47678157>.
- 41 "Remarks by President Trump on the Death of ISIS Leader Abu Bakr Al-Baghdadi," the White House, October 27, 2019, <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-death-isis-leader-abu-bakr-al-baghdadi/>.
- 42 Michael Knights and Alex Almeida, "Remaining and Expanding: The Recovery of Islamic State Operations in Iraq in 2019-2020," *CTC Sentinel* 13, No. 5 (May 2020): 12-27, <https://ctc.usma.edu/remaining-and-expanding-the-recovery-of-islamic-state-operations-in-iraq-in-2019-2020/>.
- 43 Colin Clarke and Charles Lister, "Al Qaeda Is Ready to Attack You Again," *Foreign Policy*, September 4, 2019, <https://foreignpolicy.com/2019/09/04/al-qaeda-is-ready-to-attack-you-again/>.
- 44 "Contending with ISIS in the Time of Coronavirus," *Crisis Group*; Joseph Hinks, "With the World Busy Fighting COVID-19, Could ISIS Mount a Resurgence?," *Time*, April 29, 2020, <https://time.com/5828630/isis-coronavirus/>; Ryan Browne, "ISIS Seeks to Exploit Pandemic to Mount Resurgence in Iraq and Syria," CNN, May 8, 2020, <https://www.cnn.com/2020/05/07/politics/isis-coronavirus-iraq-syria/index.html>; Ivano di Carlo, "In Chaos, They Thrive: The Resurgence of Extremist and Terrorist Groups During the COVID-19 Pandemic," *European Policy Centre*, May 5, 2020, <https://www.epc.eu/en/Publications/In-chaos-they-thrive-The-resurgence-of-extremist-and-terrorist-group> 32c800.
- 45 Michael K. Nagata, "Taking Stock of U.S. Counterterrorism Efforts Since 9/11," Washington Institute for Near East Policy, July 10, 2018, <https://www.washingtoninstitute.org/policy-analysis/view/policy-forum-july-10-2018>.

- 46 Nathan A. Sales, *After the Caliphate: A New Global Approach to Defeating ISIS*, Brookings Institution, April 30, 2019, <https://www.brookings.edu/wp-content/uploads/2019/04/20190430-Amb.-Nathan-Sales-speech-at-Brookings.pdf>.
- 47 From 2009 to 2018, Right-wing extremism was responsible for 73.3 percent of all extremist murders, compared to 23.4 percent by Islamist extremism. *Murder and Extremism in the United States in 2018*, Anti-Defamation League, January 2019, 16, <https://www.adl.org/media/12480/download#page=16>; Vera Bergengruen and W.J. Hennigan, "'We Are Being Eaten From Within.' Why America Is Losing the Battle Against White Nationalist Terrorism," *Time*, August 8, 2019, <https://time.com/5647304/white-nationalist-terrorism-united-states/>.
- 48 US Department of Homeland Security, *Department of Homeland Security 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#page=15.
- 49 US Department of Homeland Security, *Strategic Framework*, 2019.
- 50 Thomas S. Warrick, "DHS's new counterterrorism strategy calls out white supremacism, but will need resources and support," *New Atlanticist*, Atlantic Council, September 23, 2019, <https://www.atlanticcouncil.org/blogs/new-atlanticist/dhss-new-counterterrorism-strategy-calls-out-white-supremacism-but-will-need-resources-and-support/>.
- 51 Johns Hopkins University of Medicine, retrieved July 31, 2020, <https://coronavirus.jhu.edu>.
- 52 This is citing University of Washington data and models. Cecelia Smith-Schoenwalder, "Coronavirus Model Decreases Death Projection as Mask Wearing Increases," *U.S. News & World Report*, July 22, 2020, <https://www.usnews.com/news/health-news/articles/2020-07-22/coronavirus-model-decreases-death-projection-as-mask-wearing-increases>.
- 53 Derived from the 1991 US Army leadership strategic vision "Our purpose is to fight and win America's wars—anywhere, at any time, under any condition." From Gordon R. Sullivan, *The Collected Works 1991-1995*, 442, 1996, <https://babel.hathitrust.org/cgi/pt?id=mdp.39015038533942&view=1up&seq=442&q1=fight%20and%20win%20America%27s%20wars>.
- 54 DHS's lead for "non-military threats" is not intended to change the FBI's lead for federal criminal investigations, including for counterterrorism, and the DOJ lead for prosecutions of violations of federal law. Counterterrorism should be a shared mission space, in which the FBI focuses on disruptions and criminal investigations and DHS focuses on prevention and non-prosecutorial outcomes, such as working with local communities on Countering Violent Extremism or Terrorism Prevention programs. Similarly, organized crime will primarily be a domestic law enforcement priority, with DHS and the Drug Enforcement Administration both having responsibility for trying to stop narcotics from entering the United States.
- 55 Calculated using the University of Washington data and models, see Cecelia Smith-Schoenwalder, "Coronavirus," showing 77,000 more American deaths. The 9/11 death toll of 2,981 from Kean and Hamilton, *9/11 Commission Report*. https://www.navy.mil/submit/display.asp?story_id=107045.
- 56 U.S. Cyberspace Solarium Commission, *Report*, pg. 105, March 2020, <https://s.wsj.net/public/resources/documents/CSC%20Final%20Report.pdf#page=112>.
- 57 Chertoff, "Hijacking of Homeland Security," 2020.
- 58 Pew Research Center, *Public Holds Broadly Favorable Views of Many Federal Agencies, Including CDC and HHS*, April 9, 2020, <https://www.pewresearch.org/politics/2020/04/09/public-holds-broadly-favorable-views-of-many-federal-agencies-including-cdc-and-hhs/>. Views of ICE were split along partisan lines: 77 percent of Republicans had favorable views compared to only 28 percent of Democrats.
- 59 Margo Schlanger, "Offices of Goodness: Influence Without Authority in Federal Agencies," *Cardozo L. Rev.* 36, no. 1 (2014): 53-117, <https://repository.law.umich.edu/articles/1258/>.
- 60 50 U.S.C. § 3021(c)(1).
- 61 Homeland Security Presidential Directive 5, *Management of Domestic Incidents*, February 28, 2003, <https://www.dhs.gov/sites/default/files/publications/Homeland%20Security%20Presidential%20Directive%205.pdf>.
- 62 Homeland Security Act of 2002, 6 U.S.C. § 112(c), Coordination with Non-Federal Entities, <https://www.law.cornell.edu/uscode/text/6/112>.
- 63 *2010 Quadrennial Homeland Security Review Report*, Executive Summary, pg 13.
- 64 Homeland Security Presidential Directive 5; *Management of Domestic Incidents*
- 65 Jonathan Allen, "Trump's war between the states creates eBay-like fight for aid," *NBC News*, March 31, 2020, <https://www.nbcnews.com/politics/white-house/trump-s-war-between-states-creates-ebay-fight-aid-n1173116>.
- 66 S. 754 (114th): Cybersecurity Information Sharing Act of 2015.
- 67 Homeland Security Act of 2002, 6 U.S.C. § 131, Title II, Section 202.
- 68 DHS US-Cert Alert, *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems*, July 23, 2020, <https://us-cert.cisa.gov/ncas/alerts/aa20-205a>.
- 69 *2014 Quadrennial Homeland Security Review*, Natural Disasters, Pandemics, and Climate Change, pg 22.
- 70 FEMA, "Public Assistance Building Back Better," May 2018, https://www.fema.gov/media-library-data/1528733063847-314574fb8901f484e5578e5da0c9451d/PAFactSheet_BuildingBackBetterMAY2018.pdf.
- 71 *Defense Industrial Base Sector Specific Plan*, An Annex to the National Infrastructure Protection Plan, 2010, <https://www.cisa.gov/sites/default/files/publications/nipp-ssp-defense-industrial-base-2010-508.pdf>.
- 72 U.S. Cyberspace Solarium Commission, *Report*, pg. 97, <https://s.wsj.net/public/resources/documents/CSC%20Final%20Report.pdf#page=104>.

Future of DHS Project: Key Findings and Recommendations

- 73 Robert K. Knake, *Sharing Classified Cyber Threat Information with the Private Sector*, Council on Foreign Relations, May 15, 2018, <https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector>.
- 74 Wallace et al., letter to President Donald J. Trump, *Transforming the US Cyber Threat Partnership* (Draft), National Infrastructure Advisory Council, December 12, 2019, <https://www.cisa.gov/sites/default/files/publications/NIAC-Working-Group-Report-DRAFT-508.pdf>.
- 75 National Institute of Building Sciences, *Natural Hazard Mitigation Saves: 2019 Report*, December 2019, https://cdn.ymaws.com/www.nibs.org/resource/resmgr/reports/mitigation_saves_2019/mitigationsaves2019report.pdf.
- 76 U.S. Cyberspace Solarium Commission, *Report*, pg. 61, https://s.wsj.net/public/resources/documents/CSC_Final_Report.pdf - page=68.
- 77 U.S. Cyberspace Solarium Commission, *Report*, pg. 101, <https://s.wsj.net/public/resources/documents/CSC%20Final%20Report.pdf#page=108>.
- 78 Bruce Schneier, "Who Are the Shadow Brokers?," *The Atlantic*, May 23, 2017, <https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/>.
- 79 Chertoff, "Hijacking of Homeland Security," 2020.
- 80 Office of Personnel Management, *Federal Employment Viewpoint Survey*, 2019, <https://www.opm.gov/fevs/reports/governmentwide-reports/governmentwide-management-report/governmentwide-report/2019/2019-governmentwide-management-report.pdf>.
- 81 Partnership for Public Service, *Best Places to Work in the Federal Government*, 2019, retrieved July 24, 2020, <https://bestplacetowork.org>.
- 82 The three questions are "I recommend my organization as a good place to work" (currently question forty), "Considering everything, how satisfied are you with your job?" (question sixty-nine), and "Considering everything, how satisfied are you with your organization?" (question seventy-one). *Best Places to Work in the Federal Government*, 2019.
- 83 Statement by a retired US military reservist with service in the Middle East to the project director, fall 2019.
- 84 Office of Personnel Management, *FedScope*, https://www.fedscope.opm.gov/ibmcognos/bi/v1/dispatch?b_action=powerPlayService&m_encoding=UTF-8&BZ=1AAABIPUHIJ942n1OwW6CQBT8mX3YHmrePsSyBw7rshtpWrDCvaG4GIPYNUoP~n0DHGw9dCYvmcybSSYoi3IZFVudpcml92ebpQ9AdEQVay1CEROPFlxoqfjzwyi1ZR8aRQQPQZDV8utWm9ktU6ATONdb10PZPa_3dkzRCtYoKs7C2E629TNV32wlv~dnVp~7azrZxCIQOY0ff7GbykgfALCI29ngZCQi6EXpKWaqyLPtaqyls~lm07_6wSr92SPyDgico6MMWQRMkl2kDF5sK65AiHQDghl2wKKV9~U~dG7O5sBxUAhAlkO9AkkJoPfDDYCKBziv8BHjmoaM940YclP2TBmOg%3D%3D.
- 85 Zack Budryk, "Homeland Security official who rolled back some terrorism programs resigns: report," *The Hill*, October 2, 2019, <https://thehill.com/homenews/administration/464075-homeland-security-official-who-rolled-back-some-terrorism-programs>.
- 86 DHS, *Leadership*, retrieved July 25, 2020, <https://www.dhs.gov/leadership>.
- 87 Hamed Aleaziz, "'Disturbing and Demoralizing': DHS Employees Are Worried the Portland Protest Response Is Destroying Their Agency's Reputation," *BuzzFeed News*, July 21, 2020, <https://www.buzzfeednews.com/article/hamedaleaziz/dhs-employee-anger-over-portland-protest-response>.
- 88 ICF Incorporated, LLC, *Final Findings and Recommendations*, May 2019, 2, https://www.tsa.gov/sites/default/files/tsa_blue_ribbon_panel_report_execsum.pdf.
- 89 *The TSA Workforce Crisis: A Homeland Security Risk*, US House Committee on Homeland Security Subcommittee on Transportation and Maritime Security, 116th Cong. (2019) (statement of Jeffrey Neal, senior vice president ICF and chair, Blue Ribbon Panel Reviewing TSA Human Capital Service), May 21, 2019, <https://homeland.house.gov/imo/media/doc/Testimony-Neal.pdf>.
- 90 ICF Inc., *Final Findings and Recommendations*, 2019.
- 91 Joe Davidson, "Border Patrol union advocates overtime changes that would cut officers' pay," *Washington Post*, December 3, 2013, https://www.washingtonpost.com/politics/federal_government/border-patrol-union-advocates-overtime-changes-that-would-cut-officers-pay/2013/12/03/6f0fbe08-5c56-11e3-be07-006c776266ed_story.html.
- 92 Davidson, "Border Patrol overtime changes," 2013.
- 93 Davidson, "Border Patrol overtime changes," 2013.
- 94 Garrett M. Graff, "The Border Patrol Hits a Breaking Point," *Politico*, July 15, 2019, <https://www.politico.com/magazine/story/2019/07/15/border-patrol-trump-administration-227357>.
- 95 A.C. Thompson, "Years Ago, the Border Patrol's Discipline System Was Denounced as 'Broken.' It's Still Not Fixed," *ProPublica*, June 20, 2019, <https://www.propublica.org/article/border-patrol-discipline-system-was-denounced-as-broken-still-not-fixed>.
- 96 Homeland Security Advisory Council, *Final Report of the CBP Integrity Advisory Panel*, March 15, 2016, <https://assets.documentcloud.org/documents/2761266/HSAC-CBP-IAP-Final-Report-DRAFT-FINAL.pdf>.
- 97 Graff, "Border Patrol."
- 98 Ibid.
- 99 Ibid.
- 100 Ibid.
- 101 Senate Resolution 280, *Commending the Officers and Personnel of U.S. Customs and Border Protection for Their Work During the Crisis at the Southern Border*, July 23, 2019, <https://www.congress.gov/116/crec/2019/07/23/modified/CREC-2019-07-23-pt1-PgS5016.htm>.
- 102 *Assessing the Adequacy of DHS Efforts to Prevent Child Deaths in Custody*, House Homeland Security Subcommittee on Border Security, Facilitation and Operations, 116th Cong. (2020) (testimony of Brian S. Hastings, chief of law enforcement operations, US Border Patrol, US

- Customs and Border Protection), January 14, 2020, <https://www.cbp.gov/about/congressional-resources/testimony/written-testimony-brian-hastings-CHS-BSFO>.
- 103 Justin Rohrllich, “US border officers die by suicide 30% more often than other cops,” Quartz.com, October 31, 2019, <https://qz.com/1738901/us-border-officers-die-by-suicide-30-percent-more-often-than-other-cops/>, quoting a CBP document, *CBP Employee Suicide Report, Data from 2007 -Present*, September 11, 2019, <https://www.documentcloud.org/documents/6534877-Suicide-Summary-20190911-1.html>.
- 104 “Border Patrol Suicide Rate Spikes,” CBS News, August 16, 2010, <https://www.cbsnews.com/news/border-patrol-suicide-rate-spikes/>.
- 105 Customs and Border Protection, *CBP Suicide Prevention Event*, September 16, 2015, <https://www.flickr.com/photos/cbphotos/albums/72157658329738120>.
- 106 *Department of Homeland Security Morale*, House Homeland Security Committee, 116th Cong. (2020) (testimony of Angela Bailey, chief human capital officer, DHS), January 14, 2020, <https://homeland.house.gov/imo/media/doc/Testimony-Bailey.pdf>.
- 107 US Department of Homeland Security, *Joint Requirements Council*, retrieved July 27, 2020, <https://www.dhs.gov/joint-requirements-council>.
- 108 Danielle E. Gaines, “Lab at Fort Detrick Faces Closing Under Proposed Federal Budget,” *Frederick News Post*, May 24, 2017, https://www.fredericknewspost.com/news/politics_and_government/lab-at-fort-detrick-faces-closing-under-proposed-federal-budget/article_8fdc3d0d-856c-58f1-b995-7869630b6a67.html.
- 109 Danielle E. Gaines and Kate Masters, “House Passes National Spending Bill That Restores Funding to Fort Detrick Lab,” *Frederick News Post*, September 15, 2017, https://www.fredericknewspost.com/news/politics_and_government/house-passes-national-spending-bill-that-restores-funding-to-fort-detrick-lab/article_9d38ae45-4787-502a-b494-7b624e33a87f.html; and “Funding restored to National Biodefense Analysis and Countermeasures lab,” *Homeland Security News*, April 2, 2018, <http://www.homelandsecuritynewswire.com/dr20180402-funding-restored-to-national-biodefense-analysis-and-countermeasures-lab>.
- 110 S&T Public Affairs, *News Release: DHS Initiating Crucial Research to Mitigate COVID-19*, March 25, 2020, <https://www.dhs.gov/science-and-technology/news/2020/03/25/news-release-dhs-initiating-crucial-research-mitigate-covid-19>.
- 111 Government Accountability Office, *Homeland Security – Clearer Roles and Responsibilities for the Office of Strategy, Policy, and Plans and Workforce Planning Would Enhance Its Effectiveness*, September 2018, 21, <https://www.gao.gov/assets/700/694576.pdf#page=25>.
- 112 David Shaw et al., *Letter to The Honorable Kirstjen Nielsen*, undated but written June 2018, retrieved July 27, 2020, <https://www.documentcloud.org/documents/4562896-FILE-3286.html#document/p1>. See Nick Miroff, “Seeking a split from ICE, some agents say Trump’s immigration crackdown hurts investigations and morale,” *Washington Post*, June 28, 2018, https://www.washingtonpost.com/world/national-security/seeking-split-from-ice-agents-say-trumps-immigration-crackdown-hurts-investigations-morale/2018/06/28/7bb6995e-7ada-11e8-8df3-007495a78738_story.html.
- 113 Niels Lesniewski, “White House budget plan has Secret Service back under Treasury,” Roll Call, February 10, 2020, <https://www.rollcall.com/2020/02/10/white-house-budget-plan-has-secret-service-back-under-treasury/>.
- 114 Zolan Kanno-Youngs and Alan Rappeport, “Report Says Secret Service Return to Treasury Could Harm Homeland Security,” *New York Times*, January 17, 2020, <https://www.nytimes.com/2020/01/17/us/politics/secret-service-treasury-homeland-security.html>.
- 115 Carrie F. Cordero, *Reforming the Department of Homeland Security Through Enhanced Oversight & Accountability*, Center for a New American Security, May 2020, 22, <https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Report-HomelandSecurity-final-updated-060820-web-2.pdf?#page=25>.
- 116 “US Department of Justice, Organization, Mission & Functions Manual: Attorney General, Deputy and Associate,” United States Department of Justice, last updated September 9, 2014, <https://www.justice.gov/jmd/organization-mission-and-functions-manual-attorney-general>.
- 117 The need for oversight and accountability of DHS’s law enforcement operations is discussed in more detail in Cordero, *Reforming the Department of Homeland Security*, 2020.
- 118 DHS Office of the Press Secretary, *Secretary Nielsen Announces the Establishment of the Countering Weapons of Mass Destruction Office*, December 7, 2017, <https://www.dhs.gov/news/2017/12/07/secretary-nielsen-announces-establishment-countering-weapons-mass-destruction-office>.
- 119 *Examining the Department of Homeland Security’s Efforts to Counter Weapons of Mass Destruction*, Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response and Communications (testimony of James F. McDonnell, William Bryan, and Chris P. Currie, Joint Prepared Statement), December 7, 2017, 9, <https://www.hsdl.org/?view&did=812353#page=13>.
- 120 Public Law 115-387, signed by President Trump on December 21, 2018. The mission of the office is at 6 U.S.C § 591g.
- 121 Congressional testimony about the reasons why CWMD was set up does not even mention the word pandemic or influenza. *Examining the Department of Homeland Security’s Efforts to Counter Weapons of Mass Destruction*, House Homeland Security Committee Subcommittee on Emergency Preparedness, Response, and Communication, December 7, 2017, <https://www.hsdl.org/?view&did=812353>.

Future of DHS Project: Participant Biographies

Senior Advisory Board Co-Chairs



Secretary Michael Chertoff

*Executive Chairman and Co-Founder
Chertoff Group*

As secretary of homeland security from 2005 to 2009, 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, 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 DHS, Chertoff served as a federal judge on the US 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.

Chertoff is a *magna cum laude* graduate of Harvard College (1975) and Harvard Law School (1978). From 1979-80 he served as a clerk to Supreme Court Justice William Brennan, Jr. In addition to his role at Chertoff Group, Chertoff is also Senior Of Counsel at Covington & Burling LLP, and a member of the firm's White Collar Defense and Investigations practice group.



Secretary Jeh Johnson

*Partner
Paul, Weiss, Rifkind, Wharton & Garrison, LLP*

Jeh Johnson is the former secretary of homeland security. He served in that position from December 2013 to January 2017. Following that, Johnson returned to private law practice at Paul, Weiss, Rifkind, Wharton & Garrison, LLP. Johnson has been affiliated with Paul, Weiss on and off since 1984, and became the firm's first African American partner in 1994. Johnson is also currently on the board of directors of PG&E Corporation, headquartered in San Francisco, and a non-resident

Senior Fellow at the Harvard Kennedy School. Johnson's career has been a mixture of public service and private corporate law practice; he has served in three presidentially appointed Senate-confirmed positions.

Prior to becoming secretary of homeland security, Johnson was general counsel of the Department of Defense (2009-2012). In that position, Johnson is credited with being the legal architect for the US military's counterterrorism efforts in the Obama administration. In 2010, Johnson also co-authored the report that paved the way for the repeal of the Don't Ask, Don't Tell policy by Congress later that year. In October 1998, Johnson was appointed by President Clinton to be general counsel of the Department of the Air Force and served in that position until January 2001. Earlier in his career, Johnson was an assistant United States attorney for the Southern District of New York (1989-1991).

Johnson is a fellow in the American College of Trial Lawyers and a member of the Council on Foreign Relations. He is a graduate of Morehouse College (1979) and Columbia Law School (1982), and the recipient of nine honorary degrees.

Senior Advisory Board Members



Secretary Janet Napolitano

Professor of Public Policy

Goldman School of Public Policy, University of California, Berkeley

Janet Napolitano served as secretary of homeland security from January 2009 to September 2013. As University of California president from 2013 to 2020, she was a steadfast advocate for California students, working to stabilize in-state tuition and to enroll historic numbers of California undergraduates. In 2017, under Napolitano's leadership, the University of California was the first university in the country to file a lawsuit to stop the federal government's rescission of the DACA program. The injunctions the University received prohibiting the rescission of DACA were upheld by the US Supreme Court. Napolitano also upheld the university's legacy of leadership on global climate action.

As governor of Arizona from 2003 to 2009, she was the first woman to chair the National Governors Association, was named one of the nation's top five governors by Time magazine, and was named by Forbes magazine as one of the 10 most powerful women in the world. She also served as attorney general of Arizona from 1998 to 2003, and as US attorney for the District of Arizona from 1993 to 1997. Before that, she practiced at the law firm of Lewis & Roca in Phoenix, where she became a partner in 1989. She began her career in 1983 as a clerk for Judge Mary M. Schroeder of the US Court of Appeals for the Ninth Circuit.

The recipient of numerous awards and honors, Napolitano was awarded the Woodrow Wilson Award for Public Service by the Woodrow Wilson Center for Scholars at the Smithsonian Institution in 2006. In 2012, she received the Anti-Defamation League's William and Naomi Gorowitz Institute Service Award, which is given for outstanding achievements in combating terrorism, extremism and injustice. A New York City native, Napolitano grew up in Pittsburgh, PA, and Albuquerque, NM. She earned a BA degree *summa cum laude* in 1979 from Santa Clara University, where she was *Phi Beta Kappa*, a Truman Scholar, and the university's first female valedictorian. She received her JD degree in 1983 from the University of Virginia School of Law. In 2010, she was awarded the prestigious Thomas Jefferson Foundation Medal (Law), the University of Virginia's highest external honor.



Acting Secretary Rand Beers

Senior Fellow

Middle East Institute

Rand Beers served as deputy assistant to the president and deputy homeland security advisor on the National Security Council staff of the White House from January 2014 to March 2015. Beers served as acting secretary of homeland security from September 2013 to December 2013. He also served as acting deputy secretary from May 2013 until September 2013. In June 2009, Beers was nominated by President Barack Obama and confirmed by the US Senate to serve as the under secretary for the National Protection and Programs Directorate at DHS, later renamed as the Cybersecurity and Infrastructure Security Agency. He led integrated efforts to reduce risks to physical, cyber and communications infrastructures.

During his tenure at DHS before becoming the acting secretary, he concurrently served as the department's counterterrorism coordinator, overseeing departmental operational and policy functions to prevent, respond to, and mitigate threats to US national security from acts of terrorism. Throughout his service at DHS, Beers was a top advisor to the secretary of homeland security, providing counsel and guidance on a wide spectrum of homeland security issues, from counterterrorism efforts to cybersecurity. Before serving in DHS, he was the co-chair of the DHS transition team for the incoming Obama administration and served in senior positions at the Department of State.

Prior to the Obama administration, Beers was the president of the National Security Network, a network of experts seeking to foster discussion of progressive national security ideas around the country, and an adjunct lecturer at the Kennedy School of Government at Harvard. Rand Beers began his professional career as a Marine Corps officer and rifle company commander in Vietnam (1964-1968). He entered the foreign service in 1971 and transferred to the civil service in 1983.



Acting Secretary Kevin K. McAleenan

*Co-founder & Chairman
Panigam*

Kevin McAleenan served as acting secretary of homeland security from April to October 2019. Before this appointment, he served as commissioner of US Customs and Border Protection (CBP), having been confirmed by the US Senate in March 2018. Previously, he had served as CBP acting commissioner since January 2017. As CBP's chief executive, McAleenan oversaw 60,000 employees and managed a budget of more than \$13 billion. Previously, McAleenan served as deputy commissioner from November 2014, until his appointment to acting commissioner. In this role, he served as the agency's chief operating officer and senior career official.

From 2006 to 2008, McAleenan served as the area port director of Los Angeles International Airport, directing CBP's border security operations at the Los Angeles airport and 17 other airport facilities in one of CBP's largest field commands. In December 2011, he was named acting assistant commissioner of CBP's Office of Field Operations. In this position, McAleenan led agency operations to secure the US border while expediting lawful trade and travel at 329 ports of entry in the United States and 70 international locations in more than 40 countries.

McAleenan received a 2015 Presidential Rank Award—the nation's highest civil service award. In 2005, he received the Service to America Medal, and the Call to Service Award, for spearheading efforts to develop and implement a comprehensive antiterrorism strategy in the border security context after Sept. 11, 2001. He received his Juris Doctor degree from the University of Chicago Law School and a Bachelor of Arts degree from Amherst College.

Report Authors



Thomas S. Warrick

*Director, Future of DHS Project
and Nonresident Senior Fellow, Scowcroft Center for Strategy and Security
Atlantic Council*

Tom Warrick is a nonresident senior fellow at the Atlantic Council. Prior to joining the Atlantic Council, from August 2008 to June 2019 he was the deputy assistant secretary for counterterrorism policy at the US Department of Homeland Security and a career member of the Senior Executive Service. He was an international lawyer in private practice for 17 years, representing companies in connection with investments in the Middle East and elsewhere.

From 1997 to 2007, he served in the US Department of State on Middle East and international justice issues. From 1997 to 2001, Warrick was deputy in the Office of the Secretary / Office of War Crimes Issues. In 2001, he became special adviser, then senior adviser, to the assistant secretary of state for Near Eastern Affairs, working on Iraq, Iran, and other issues. From 2002 to 2003, he led the State Department's "Future of Iraq" project. From October 2003 to June 2006, he served in both Baghdad and Washington. From July 2006 to July 2007, he was director (acting) for Iraq Political Affairs. He was briefly senior political adviser on the Iran desk in 2007.

Warrick joined the US Department of Homeland Security in August 2007 as director for the Middle East, Africa, and South Asia in the Office of Policy. He became deputy assistant secretary for counterterrorism policy, in the Office of Policy, in August 2008. In February 2015, Warrick was named deputy counterterrorism coordinator for policy by the DHS counterterrorism coordinator and under secretary for Intelligence & Analysis. In July 2018, when the counterterrorism policy mission was returned to the DHS Office of Policy, Warrick resumed his title of deputy assistant secretary for counterterrorism policy in the Office of Policy / Office of Threat Prevention and Security Policy. Warrick concluded his service as Deputy Assistant Secretary for Counterterrorism Policy on June 14, 2019. Warrick received his Juris Doctor degree from Harvard Law School in 1979 and a Bachelor of Science in Public Administration *summa cum laude* from the University of Missouri.

For the Department of Homeland Security and the State Department, Warrick has worked on national strategies involving counterterrorism, Iran, defeating ISIS, Iraq, Syria, Turkey, Lebanon, Egypt, South Asia, Africa, West Africa Counterterrorism, Somalia, Lebanese Hezbollah, Afghanistan, Pakistan, Israeli-Palestinian affairs, countering terrorist propaganda, Terrorist Travel, Terrorist Use of the Internet, and Russia.



Caitlin Durkovich

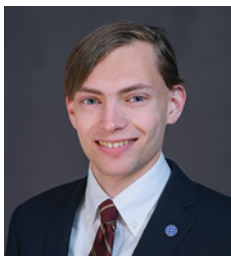
*Co-Director, Future of DHS Project and Nonresident Senior Fellow,
Scowcroft Center for Strategy and Security
Atlantic Council;
Director
Toffler Associates*

Caitlin Durkovich is a nonresident senior fellow in the Scowcroft Center for Strategy and Security and a director at Toffler Associates. She has more than twenty years of expertise in national and homeland security. A recognized expert in critical infrastructure security and resilience, including cybersecurity, Durkovich has successfully advanced risk management programs that drive thought leadership, advance leading security practices, influence policy, and evolve industry practices to manage operational and security risks. She has advanced strategy and policy at the highest levels of government, including the development of Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (2013) and cochairing the Joint United States-Canada Electric Grid Security and Resilience Strategy (2016) and the National Space Weather Strategy (2015).

Durkovich is a director at Toffler Associates, a foresight advisory firm. She served eight years at the Department of Homeland Security, managing the mission to protect the nation's cyber and physical infrastructure. As assistant secretary for infrastructure protection, she led both the voluntary partnership to enhance security and resilience across the sixteen critical infrastructure sectors, as well as the regulatory program to secure high-risk chemical facilities, or the Chemical Facility Antiterrorism Standards (CFATS). Her experience also includes leading homeland security projects with several government agencies while at Booz Allen Hamilton, setting industry cybersecurity standards at the ISAlliance, and pioneering early warning cyber intelligence at iDefense (acquired by Verisign). Durkovich is a member of the Board of Directors of the InfraGard National Members Alliance and the Protect Our Power Advisory panel.

She earned a BA in public policy studies from the Terry Sanford Institute of Public Policy at Duke University and a certificate in business strategy from The Aspen Institute. She lives in Washington, DC with her husband, three children, and bulldog.

Project and Research Support



Mark J. Massa

*Program Assistant, Forward Defense, Scowcroft Center for Strategy and Security
Atlantic Council*

Mark J. Massa is a program assistant in *Forward Defense* within the Scowcroft Center for Strategy and Security at the Atlantic Council. Massa contributes to *FD* programs and research on nuclear security and arms control, homeland security, the Commanders Series, and other endeavors. He is a second-year MA candidate in the Security Studies Program at the Georgetown University School of Foreign Service. His research focuses on nuclear weapons, emerging technology, and the Arctic.

Massa graduated *magna cum laude* from Georgetown University with a degree in Science, Technology, and International Affairs.

Acknowledgements

The following individuals participated in the Future of DHS Project study groups or otherwise contributed to the report. Current and former affiliations are listed for informational purposes only, as all contributors participated in an individual, not institutional, capacity. The authors maintain all responsibility for the content of the report.

Ms. Susan Aarons

Lead Associate, Justice Homeland Transportation
Booz Allen Hamilton;
Former Special Agent, National Security, Immigration and Customs Enforcement
US Department of Homeland Security

Mr. Javed Ali

Towsley Policymaker in Residence
University of Michigan Gerald R. Ford School of Public Policy

Mr. Stewart Baker

Step toe & Johnson LLP;
Former Assistant Secretary for Policy
US Department of Homeland Security

Mr. Patrick Barry

Executive
General Dynamics Information Technology

Mr. Christian Beckner

Senior Director, Retail Technology and Cybersecurity
National Retail Foundation;
Former Associate Staff Director
Senate Homeland Security and Governmental Affairs Committee

Mr. Christopher J. Boyer

Vice President, Global Security & Technology Policy
AT&T Inc.

Mr. Chuck Brooks

Adjunct Faculty, Program in Applied Intelligence
Georgetown University

Mr. Nate Bruggeman

Principal
BorderWorks Advisors LLC;
Formerly Counselor to the Commissioner, Customs and Border Protection
US Department of Homeland Security

Mr. Thomas J. Bruno

Managing Director, Department of Homeland Security Account
Accenture Federal Services***

Mr. Stevan E. Bunnell

Chief Legal Officer
Libra Association;
Former General Counsel
US Department of Homeland Security

Ms. Britaini S. Carroll

Human Capital Principal Director, Workforce Transformation
Accenture Federal Services***

Mr. Steven A. Cash

Counsel
Day Pitney LLP

Mr. John D. Cohen

Senior Expert on Global Threats
Argonne National Laboratory;
Former Acting Under Secretary for Intelligence and Analysis
US Department of Homeland Security

Ms. Kathryn Condello

Senior Director, National Security & Emergency Preparedness
CenturyLink

Ms. Carrie Cordero

Robert M. Gates Senior Fellow
Center for a New American Security

Mr. Chris Cummiskey

Chief Executive Officer
Cummiskey Strategy Solutions LLC;
Former Deputy Under Secretary for Management
US Department of Homeland Security

Mr. Lawrence Curran

Data Scientist and Project Manager
New Light Technologies Inc.;
Former Section Chief, Secretary's Briefing Staff
US Department of Homeland Security

Mr. Brian de Vallance

Senior Fellow, McCrary Institute for Cyber and Critical Infrastructure Security
Auburn University;
Former Assistant Secretary for Legislative Affairs
US Department of Homeland Security

Mr. John F. Dermody

Counsel
O'Melveny & Myers, LLP

Dr. J. Bradley Dickerson

Senior Manager
Sandia National Laboratories;
Former Director of Chemical Security Policy and Senior Biodefense Advisor
US Department of Homeland Security

Ms. Marjorie Dickman

Chief Government Affairs and Public Policy Officer
BlackBerry Corporation

Dr. Holly A. Dockery

Deputy Vice President, International, Homeland, and Nuclear Security
Sandia National Laboratories

* Atlantic Council Member ** Atlantic Council Board Director*** Atlantic Council Corporate Member

Mr. Thomas R. Eldridge**

Senior Vice President, Strategic Development
SAIC***

Mrs. Marsha (Catron) Espinosa

Chief of Staff
Office of U.S. Rep. Linda Sánchez

Ms. Maurine Fanguy

Managing Director, Department of Homeland Security Account
Accenture Federal Services***

Mr. Thomas A. Fanning

Chairman, President, and CEO
Southern Company

Mr. Andrew Farnsworth

Intern, Forward Defense, Scowcroft Center for Strategy and Security
Atlantic Council

Mr. Patrick Flanagan

Co-Founder
Pre LLC

Mr. A.J. Gary

Homeland Security Advisor and Director
Arkansas Division of Emergency Management

Dr. Daniel M. Gerstein

Senior Policy Researcher
RAND Corporation;
Former Under Secretary (Acting) and Deputy Under Secretary, Science and Technology Directorate
US Department of Homeland Security

Dr. Robert P. (Bob) Griffin Jr.

Founding Dean, College of Emergency Preparedness, Homeland Security, and Cyber Security
State University of New York at Albany

Ms. Michele L. Guido

Strategic Security Policy Director
Southern Company

Dr. Trey Herr

Director, Cyber Statecraft Initiative, Scowcroft Center for Strategy and Security
Atlantic Council

Mr. David F. Heyman

CEO & Co-Founder
Smart City Works VENTURE Labs;
Former Assistant Secretary for Policy
US Department of Homeland Security

Mr. Jason Houser

Senior Instructor, Political Science
United States Naval Academy;
Former Deputy Chief of Staff of Intelligence
US Department of Homeland Security

Lt Col Chris Kelenske

Deputy Homeland Security Advisor to Michigan Governor Gretchen Whitmer and Deputy Director
Michigan State Police

Mr. Kevin R. Klein

Director
Colorado Division of Homeland Security and Emergency Management

Ms. Connie LaRossa

Principal
Cornerstone Government Affairs

Dr. Chappell Lawson

Associate Professor, Political Science
Massachusetts Institute of Technology

Mr. Jonathan Lee

Director, Global Public Policy
WhatsApp Inc.***

Amb. (ret.) Marisa Lino

Adjunct Political Scientist
RAND Corporation;
Former Assistant Secretary for International Affairs
US Department of Homeland Security

Mr. Andrew Lorenzen-Strait

Managing Director and Founder
Lorenzen-Strait Consulting Services, LLC;
Former Deputy Assistant Director, Immigration and Customs Enforcement
US Department of Homeland Security

Mr. Timothy Manning

Non-Resident Senior Fellow, Adrienne Arsht – Rockefeller Foundation Center for Resilience
Atlantic Council;
Former Deputy Administrator for Protection and National Preparedness, Federal Emergency Management Agency
US Department of Homeland Security

Mr. Charles Marino

Chief Executive Officer
Sentinel Security Solutions, LLC

Mr. Philip A. McNamara

Director, Government Relations
Pew Charitable Trusts;
Former Assistant Secretary for Intergovernmental Affairs, Partnerships, and Engagement
US Department of Homeland Security

Mr. Coleman Mehta

Senior Director, U.S. Policy
Palo Alto Networks, Inc.;
Former Director, Legislative Affairs
US Department of Homeland Security

Mr. Ian S. Mitch

Senior Policy Analyst
RAND Corporation

LTG Michael K. Nagata, USA (Ret.)

Senior Advisor to the Senior Vice President
CACI International Inc.

VADM Peter Neffenger, USCG (Ret.)

Distinguished Fellow, Adrienne Arsht - Rockefeller Foundation Center for Resilience
Atlantic Council

*Atlantic Council Member **Atlantic Council Board Director ***Atlantic Council Corporate Member

Future of DHS Project: Key Findings and Recommendations

Mr. Roger Parrino, Sr.

Director of Preparedness, Intelligence, and Inspections
Port Authority of New York and New Jersey

Mr. Barry Pavel

Senior Vice President and Director, Scowcroft Center for Strategy and Security
Atlantic Council

Mr. Timothy Perry

Chief of Staff and Deputy Homeland Security Advisor
California Governor's Office of Emergency Services

Ms. Briana Petyo Frisone

National Security Sector Advisor
Guidehouse;
Former Counselor to the Acting Secretary
US Department of Homeland Security

Mr. Thomas K. Plofchan, III

Managing Partner
Pangiam;
Former Counterterrorism Counselor to the Secretary
US Department of Homeland Security

Ms. Amy E. Pope

Non-Resident Senior Fellow, Adrienne Arsht - Rockefeller Foundation Center for Resilience
Atlantic Council

Ms. Amy L. Rall

Vice President, Homeland and Justice Programs
SAIC***

Ms. Subhasri "Sue" Ramanathan

Non-Resident Senior Fellow, Hume Center for National Security & Technology
Virginia Polytechnic Institute and State University;
Former Deputy Assistant Secretary and Counselor to the Secretary
US Department of Homeland Security

Mr. Jeff Ratner

Senior Manager, Global Cybersecurity and Privacy Law
Apple, Inc.

Ms. Lora Ries

Senior Research Fellow, Homeland Security
The Heritage Foundation;
Former Acting Deputy Chief of Staff
US Department of Homeland Security

Mr. Eric Rosand

Director
The Prevention Project

Mr. Paul Rosen

Partner
Crowell & Moring LLP

Ms. Laura Rosenberger

Senior Fellow and Director, Alliance for Securing Democracy
The German Marshall Fund of the United States

Mr. Todd Rosenblum

Non-Resident Senior Fellow, Scowcroft Center for Strategy and Security
Atlantic Council;
Former Deputy Under Secretary of Intelligence
US Department of Homeland Security

Mr. Paul Rosenzweig

Senior Fellow
R Street Institute

Mr. William Ruch

Principal
Lewis-Burke Associates LLC

Mr. Marc R. Sabbagh

Chief of Staff, Safety and Citizen Services
Accenture Federal Services***

Ms. Jen Sadosky

Human Capital Lead, Safety and Citizen Services
Accenture Federal Services***

Mr. Fred Schwien

Director of Homeland Security Programs and Strategy
The Boeing Company***

Ms. Suzanne Spaulding

Senior Adviser, Homeland Security, International Security Program
Center for Strategic and International Studies;
Former Under Secretary, Department of Homeland Security

Ms. Clementine Starling

Deputy Director, Forward Defense & Resident Fellow, Transatlantic Security Initiative, Scowcroft Center for Strategy and Security
Atlantic Council

Ms. Bobbie Stempfley

Vice President, Cyber Security and Business Security Officer ISG
Dell Technologies;
Former Deputy Assistant Secretary for Cybersecurity and Communications
US Department of Homeland Security

Ms. Camille Stewart

Cyber Fellow
Harvard Belfer Center for Science and International Affairs;
Former Senior Policy Advisor, Cyber, Infrastructure, & Resilience Policy
US Department of Homeland Security

Ms. Lauren Stienstra

Program Director, Homeland Security and Emergency Management
National Governors Association

Mr. Seth Stodder

Partner
Holland & Knight LLP

Mr. Steven G. Stransky

Partner
Thompson Hine LLP;
Former Deputy Legal Adviser
National Security Council

*Atlantic Council Member **Atlantic Council Board Director ***Atlantic Council Corporate Member

Mr. Philip Stupak

*Fellow, Harris Cyber Policy Initiative
University of Chicago;
Former Senior Advisor to the Deputy
Secretary
US Department of Homeland Security*

BG Francis X. Taylor, USAF (Ret.)

*Global Policy Initiative Executive Fellow
University of Notre Dame;
Former Under Secretary, Office of
Intelligence and Analysis
US Department of Homeland Security*

Mr. Miles E. Taylor

*US Lead, Advanced Technology and
Security Strategy (on leave)
Google, Inc.;
Former Chief of Staff
US Department of Homeland Security*

Mr. Scott Tousley

*Senior Executive, Cyber Programs
Splunk Inc.;
Former Deputy Director, Cybersecurity
Research, Science & Technology
Directorate
US Department of Homeland Security*

Ms. Paula Trimble

*Senior Principal
Lewis-Burke Associates LLC*

Mr. Christian Trotti

*Assistant Director, Forward Defense,
Scowcroft Center for Strategy and
Security
Atlantic Council*

Mr. Tip Underwood

*Vice President, Department of
Homeland Security Programs
SAIC****

Mr. Stephen R. Viña

*Senior Vice President and Senior
Advisory Specialist, Cyber Practice
Marsh LLC;
Former Chief Counsel for
Homeland Security
US Senate Committee on Homeland
Security and Governmental Affairs*

Mr. Peter Vincent

*Global Security Consultant;
Former Principal Legal Advisor and
Senior Counselor for International Policy,
Immigration and Customs Enforcement
US Department of Homeland Security*

Ms. Kemba Walden

*Senior Counsel, Cyber & Democracy
Microsoft Corporation;
Former Attorney-Advisor, Office of
General Counsel
US Department of Homeland Security*

Mr. Robert Walker

*Executive Director
Homeland Security Experts Group*

Ms. Erin Waters

*Communications Consultant;
Former Advisor and Director of Strategic
Communication
US Department of Homeland Security*

Mr. William F. Wechsler

*Director, Rafik Hariri Center and Middle
East Programs
Atlantic Council;
Former Deputy Assistant Secretary for
Special Operations and Combatting
Terrorism & Former Deputy Assistant
Secretary for Counternarcotics and
Global Threats
US Department of Defense*

Mr. Reza Zomorrodian

*Homeland Security Policy Analyst
National Governors Association*

*Atlantic Council Member **Atlantic Council Board Director ***Atlantic Council Corporate Member

The Future of DHS Project was made possible with generous contributions from our founding partner SAIC and an additional generous contribution from CenturyLink. The Atlantic Council is deeply grateful for their support in this effort.



CenturyLink®



CHAIRMAN

*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS

*James L. Jones

CHAIRMAN EMERITUS

Brent Scowcroft

PRESIDENT AND CEO

*Frederick Kempe

EXECUTIVE VICE CHAIRS

*Adrienne Arsht

*Stephen J. Hadley

VICE CHAIRS

*Robert J. Abernethy

*Richard W. Edelman

*C. Boyden Gray

*Alexander V. Mirtchev

*John J. Studzinski

TREASURER

*George Lund

SECRETARY

*Walter B. Slocombe

DIRECTORS

Stéphane Abrial

Odeh Aburdene

Todd Achilles

*Peter Ackerman

Timothy D. Adams

*Michael Andersson

David D. Aufhauser

Colleen Bell

Matthew C. Bernstein

*Rafic A. Bizri

Linden Blue

Philip M. Breedlove

Myron Brilliant

*Esther Brimmer

R. Nicholas Burns

*Richard R. Burt

Michael Calvey

James E. Cartwright

John E. Chapoton

Ahmed Charai

Melanie Chen

Michael Chertoff

*George Chopivsky

Wesley K. Clark

*Helima Croft

Ralph D. Crosby, Jr.

*Ankit N. Desai

Dario Deste

Paula J. Dobriansky

Joseph F. Dunford, Jr.

Thomas J. Egan, Jr.

Stuart E. Eizenstat

Thomas R. Eldridge

*Alan H. Fleischmann

Jendayi E. Frazer

Courtney Geduldig

Robert S. Gelbard

Thomas H. Glocer

John B. Goodman

*Sherri W. Goodman

Murathan Günal

*Amir A. Handjani

Katie Harbath

John D. Harris, II

Frank Haun

Michael V. Hayden

Amos Hochstein

*Karl V. Hopkins

Andrew Hove

Mary L. Howell

Ian Ihnatowycz

Wolfgang F. Ischinger

Deborah Lee James

Joia M. Johnson

Stephen R. Kappes

*Maria Pica Karp

Andre Kelleners

Astri Kimball Van Dyke

Henry A. Kissinger

*C. Jeffrey Knittel

Franklin D. Kramer

Laura Lane

Jan M. Lodai

Douglas Lute

Jane Holl Lute

William J. Lynn

Mian M. Mansha

Marco Margheri

Chris Marlin

William Marron

Neil Masterson

Gerardo Mato

Timothy McBride

Erin McGrain

John M. McHugh

H.R. McMaster

Eric D.K. Melby

*Judith A. Miller

Dariusz Mioduski

*Michael J. Morell

*Richard Morningstar

Virginia A. Mulberger

Mary Claire Murphy

Edward J. Newberry

Thomas R. Nides

Franco Nuschese

Joseph S. Nye

Hilda Ochoa-Brillembourg

Ahmet M. Ören

Sally A. Painter

*Ana I. Palacio

*Kostas Pantazopoulos

Carlos Pascual

Alan Pellegrini

David H. Petraeus

W. DeVier Pierson

Lisa Pollina

Daniel B. Poneman

*Dina H. Powell McCormick

Robert Rangel

Thomas J. Ridge

Lawrence Di Rita

Michael J. Rogers

Charles O. Rossotti

Harry Sachinis

C. Michael Scaparrotti

Rajiv Shah

Stephen Shapiro

Wendy Sherman

Kris Singh

Christopher Smith

James G. Stavridis

Richard J.A. Steele

Mary Streett

Frances M. Townsend

Clyde C. Tuggle

Melanne Verveer

Charles F. Wald

Michael F. Walsh

Gine Wang-Reese

Ronald Weiser

Olin Wethington

Maciej Witucki

Neal S. Wolin

*Jenny Wood

Guang Yang

Mary C. Yates

Dov S. Zakheim

HONORARY DIRECTORS

James A. Baker, III

Ashton B. Carter

Robert M. Gates

Michael G. Mullen

Leon E. Panetta

William J. Perry

Colin L. Powell

Condoleezza Rice

George P. Shultz

Horst Teltschik

John W. Warner

William H. Webster

**Executive Committee
Members*

List as of June 30, 2020



The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

© 2020 The Atlantic Council of the United States. All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Atlantic Council, except in the case of brief quotations in news articles, critical articles, or reviews. Please direct inquiries to:

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org