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.

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 Thomas 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. 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—infected diseases, cyber threats from hostile nation-states, threats to election security, foreign disinformation, threats to critical infrastructure from climate change, vulnerabilities from new technologies, and growing white supremacism. DHS was founded in 2003 to focus on the threat from terrorism. The department was later pushed to take on new missions without adequate resources. Today’s challenges demand more DHS leadership attention and resources, even as the department 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.¹ DHS has occupied last place in federal employee morale among large cabinet departments every year since 2010.²
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 employees and an annual budget of $62 billion. 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 needs to undertake so that it can meet the newly emerging threats that—paradoxically—DHS is the best cabinet department to address.

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

Key Findings

Covid-19 in the remaining five months of 2020 is forecast to kill twenty-five times the number of people killed on 9/11, 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 as a result. By August 2020, Covid-19 had killed more than 150,000 Americans—more than in the flu pandemics of 1967-68 and 1957-58, or US deaths in World War I. In US history, Covid-19 deaths are exceeded only by World War II, the Civil War, and the 1918-19 Spanish flu pandemic.

A faster federal government response to Covid-19 would have cut the death toll by at least half, according to at least one model. Detailed plans from 2016 to respond to a pandemic were not activated. As Figure 1 makes clear, the difference between Covid-19 cases in the United States and the European Union (EU) points to a massive US government-wide policy failure.

DHS needs to take a stronger leadership role in mobilizing resources and public support to defend the nation from Covid-19 and future pandemics.

II. 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, or 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.
Author Max Brooks caught the irony of today’s strategic situation:

“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.”

Today, there is a consensus that Russia, China, and Iran are carrying out non-kinetic attacks through nation-state cyber operations for political or financial gain; challenging US election security; attacking critical infrastructure; carrying out acts of disinformation; undermining confidence in the US judicial system; manipulating social media, including through foreign covert influence campaigns; and using other hostile nonmilitary means to weaken the country.

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 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.”

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.

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 election infrastructure using both social and traditional media. Former Vice President Joseph R. Biden, Jr., 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.”

Cyberattacks by hostile nation-states, 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 US 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 American 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. 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.

The department best suited to defend the United States against threats to democracy is DHS. DHS is already responsible for cybersecurity, critical infrastructure, and key aspects of election security. DHS is already set up for information sharing and collaboration with the primary targets of these hostile nation-state campaigns: the 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. As former DHS Deputy Secretary Jane Holl Lute often said, there are times when the US Department of Defense (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 need to be, to the greatest extent possible, “above politics.” This is essential for credibility on election security. The chairman of the Joint Chiefs of Staff and the uniformed military 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.
DHS needs to get ready for the changing terrorist threat.

DHS has a major role in preventing terrorists from entering the United States, working with local communities on countering violent extremism and terrorism prevention, and 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 recently as 2016.

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.22 Al-Qaeda in the Arabian Peninsula (AQAP) claimed credit for the December 6, 2019, terrorist attack at the Naval Air Station in Pensacola, Florida.

Domestic terrorism by white supremacists and other “homegrown” causes also needs more DHS attention and resources.

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, (2) in the long term, threats to critical infrastructure from climate change or extreme weather, and (3) starting immediately, non-military threats from nation-states like Russia, China, and Iran.

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,”23 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.24

Three urgent recommendations to address Covid-19:

1.5 DHS urgently needs to devote significantly greater leadership focus and resources to efforts against Covid-19, which has the potential to inflict additional American deaths equal to twenty-five more 9/11 attacks before the end of 2020 and will still be a major crisis in January 2021.25 DHS needs to do much more to solve the resource and logistic shortfalls that continue to occur and to harmonize states’ response efforts.

1.6 DHS needs to be more proactive in sounding the national alarm in future pandemics to ensure the federal government is fully mobilized. The failure to mobilize the federal government in early 2020 resulted in tens of thousands of avoidable deaths in the United States. This should never happen again. DHS has the ability to elevate a public health issue into a national security issue.

1.7 DHS likewise needs to ensure that national medical supply stockpiles are rebuilt quickly and that pandemic plans are kept available so they can be executed when needed.

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 Cyberspace Solarium Commission has also called for additional resources for DHS cybersecurity.

1.9 The next DHS leadership team needs to be built around a common understanding of the most urgent
Future of DHS Project

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, the private sector, and state and local governments, and, especially, DHS’s employees. DHS needs a public affairs, internal communications, and legislative affairs operation to match those of the State and Defense Departments.

1.11 DHS also needs to invest urgently in considerably wider access to classified voice and data networks used throughout the national security community. The State Department, the Treasury Department, the Department of Justice (DOJ), and the Federal Bureau of Investigation (FBI) already have this. If DHS is to lead the defense of the nation against nonmilitary 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’s missions are broad and cut across many aspects of American life. The American people need to have confidence that DHS is exercising power responsibly. That confidence cannot be commanded; it must be earned whenever DHS takes action.

II. DHS’s Unique Public-Private Partnerships 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 with many stakeholders. 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.

Climate change or extreme weather will have an increasing impact on the operational environments that DHS helps secure. Climate change also represents the most significant long-term threat to critical infrastructure. DHS is not responsible for addressing climate change, but it is responsible for getting others to protect infrastructure that is at risk.

For cyber and other threats, DHS’s ability to facilitate information-sharing between companies that are normally competitors is a vital reason why the homeland security enterprise is essential. This allows companies facing similar threats to share information and work with DHS to counter or mitigate those threats. DHS does this by providing liability and other protections when companies share information in DHS-approved channels.

Some key stakeholders, such as the financial services, telecommunications, and the electricity sectors, need higher-fidelity, often classified, intelligence to take action against threats.

Increasing the speed of sharing is now vital for both government and industry, as cyberattacks and defenses interact at network speed, and 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.

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.

Recommendations for Modernizing DHS’s Public-Private Partnerships

Overall

2.1 Task the Office of Partnership and Engagement 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 of 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. Moreover, DHS has unique authorities to convene government and private sector stakeholders to address active and emerging threats. These authorities need to be catalogued and reviewed so DHS leadership can effectively leverage partners in mitigating risk.

2.2 DHS should inventory its information-sharing relationships and adjust its practices according to the different levels and capabilities of state, local, tribal, territorial and private sector stakeholders. Information-sharing is central to DHS’s public-private partnerships, but information-sharing is not one-size-fits-all. Information should be timely and actionable. Different-sized organizations have different levels of knowledge and need different levels of detail to drive corporate executive or governmental actions. Some businesses need classified context before taking action. Some just want to be told what DHS needs them to do.

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 at the local level and needs to do more to take advantage of this sustained presence, which is often better attuned than Washington to the needs of local partners.

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, including additional security support from DHS.

2.5 DHS should ensure threats against systemically important critical infrastructure are a priority across the Intelligence Community. The US Intelligence Community’s collection priorities should include threats against critical infrastructure companies.

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. Mitigation projects can avoid as much as $6 in damage for every $1 invested. DHS’s grant programs should be more balanced toward all-hazards and encourage partners to undertake projects that build resilience against climate change, pandemics, cyberattacks, and other “nontraditional” threats; programs like the Office of Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act Implementation, should be elevated.

Cybersecurity

2.7 DHS should work with Congress to authorize and appropriate a Cyber Resilience Fund, akin to the Disaster Recovery Fund. In a crisis, there is no substitute for ready cash. Nothing undermines an adversary’s cyber offensive strategy better than a recovery that happens within hours rather than days.

2.8 DHS should support and lead the Joint Collaborative Environment for the sharing of threat information, insights, and other data across the federal government and with the private sector. This was a recommendation of the Cyberspace Solarium Commission.

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, as is the case with DOD, where the Joint Staff representative is also at the table.

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 in twelve out of thirteen Federal Employee Viewpoint Surveys (FEVS) done since 2003—and every year since 2010 (Figure 2). At the same time, DHS employees remain committed to the department and its missions. DHS’s best FEVS survey question relative to other departments is “The work I do is important.” Addressing the workplace issues that drive DHS’s low morale needs to be one of DHS’s top priorities.
DHS is a component-driven organization, which hinders the department’s ability to fully align employees to a unified mission and shared purpose.

A lack of common DHS culture and other challenges related to organizational culture and different degrees of employee engagement are holding DHS back as a department from moving toward a culture of innovation, collaboration, and empowerment.

DHS employees are focused on their component’s goals and appear not to know or understand departmental strategies or goals, nor how their individual work contributes to the larger DHS mission. On FEVS Question 56, “Managers communicate the goals of the organization,” DHS employees ranked the department fourteen out of fourteen—lowest ranked of the large cabinet departments for which FEVS reported data.

On FEVS Question 12, “I know how my work relates to agency goals” (Figure 3), Customs and Border Protection (CBP), CISA, Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and United States Secret Service (USSS) employees—74 percent of DHS—rate DHS relatively lower on whether they understand 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.
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. 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 agreed that “My organization’s senior leaders maintain high standards of honesty and integrity.” This is remarkable in a department with the security missions and functions that DHS has.

Turning around DHS’s morale problems starts with 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.33

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

**Intelligence and Analysis (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 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 scores across the board were higher than before Taylor took office.

**USSS under Secretary Kelly and Director Alles:** USSS was rocked by scandal in 2012 when agents had to be disciplined for hiring prostitutes in Cartagena, Colombia.
The decline was halted in 2016 and 2017 by DHS Secretary Jeh Johnson, then morale improved steadily from 2017 to 2019 under DHS Secretary John F. Kelly and Secretary Jeh Johnson, then morale improved steadily (Figure 6).

- **ICE under Director Sarah Saldaña** underwent an even stronger surge in employee morale from 2015 to 2017 (Figure 7).

- **USCIS is DHS’s other civilian long-term morale success story.** As of May 2019, USCIS had shown a steady, year-on-year improvement in almost all categories (Figure 8).

**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 that drive 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. 34
Listen to what DHS employees are saying:

3.4 DHS should considerably increase two-way communications with its employees. DHS leadership needs to 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. DHS needs to look for “red flags” for warning signs of changes that need to be made. 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. Allow DHS employees to transfer more easily between components. Meritorious service in an entry-level position should give employees a preference that increases a candidate's prospects for being hired elsewhere in DHS. 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.

TSA

3.7 Morale at TSA can be improved by urgently addressing issues of pay, promotions and career advancement, and employee empowerment. Apart from the much smaller I&A and Countering Weapons of Mass Destruction (CWMD) offices, in 2019, TSA was the lowest-ranked component of DHS.

TSA employees' low pay (Figure 9) is a problem that cries out for correction.

TSA has similar problems offering its employees, especially screeners, a career path with meaningful promotion and advancement (Figure 10).

Significantly, in most other respects TSA does not stand out. TSA is no exception to the rule at DHS that employees regard their immediate supervisors relatively highly (Figure 11). TSA is in the middle for matching employees to the mission, teamwork, and innovation. It is only on low pay, lack of promotion, and limited career opportunities that TSA stands out.

A separate group of experts convened by TSA Administrator David Pekoske independently reached similar conclusions.

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. This 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 the 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.
Disciplining poor performers, including discipline for those who have shown a weakness for corruption, has been a serious problem at CBP. Expansion of the Border Patrol from FY 2006 through FY 2011 led to a lowering of standards.37 A March 2016 Homeland Security Advisory Council report concluded: “The CBP discipline system is broken.”38 Investigations became turf battles between the DHS inspector general, FBI, ICE, and CBP’s internal affairs office.39

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.” 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 were undone by practices they felt were set by judges or higher officials who did not value their work. DHS needs to 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.

This may take a major change in Border Patrol culture. 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.40

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 “to offer additional counseling services to CBP officers and personnel.”41 An additional $1.1 billion in emergency supplemental funding in July 201942 helped CBP’s resource problems, but it did little to solve CBP’s other underlying problems.

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.

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. Other priorities 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.

DHS will never achieve its potential as a cabinet department until it addresses its headquarters-component problems.

- 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 it.

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

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. 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 DHS’s Office of Strategy, Policy, and Plans (PLCY) needs to devote considerably greater efforts to better communication throughout DHS operational components of national and DHS policy priorities. DHS needs to invest in a common platform for classified connectivity.

4.3 Components need to rotate personnel, including some of their best people, in tours at headquarters so that they gain headquarters experience. Half of all personnel in headquarters offices should eventually be component detailers and half should be permanent headquarters personnel. Analogous to joint duty being required in the military, serving a tour at DHS’s headquarters should be required for promotions to GS-15 or higher. Headquarters should similarly require entry-level policy officers to serve a tour with a component.

4.4 DHS should make no major reorganizational changes in the next year because the resulting disruption will take focus away from DHS’s more urgent mission and management challenges. 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. DHS shorthand for the secretary of homeland security is “S1,” with “S2” for the Deputy Secretary. Because of the breadth of DHS’s missions, DHS needs a third
senior official, “S3,” analogous to DOJ, which has a deputy attorney general who acts as the primary backup to the attorney general and oversees parts of DOJ, and an associate attorney general, who oversees the Civil Division and other offices.43

If DHS’s deputy secretary (“S2”) has a law enforcement background, that person could serve such a role—but then “S3” would need to free up some of the deputy secretary’s time to handle law enforcement coordination.

**Until Congress acts, DHS should designate a very senior DHS official to coordinate its law enforcement agencies**, analogous to the way DHS Secretary Janet Napolitano and subsequent secretaries designated a DHS under secretary to serve as the DHS counterterrorism coordinator.

**4.6 DHS should immediately return policy officials working biological, chemical, and nuclear threat issues to PLCY** to support DHS’s urgent and ongoing response to the Covid-19 pandemic in 2021.

**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 was killing as many Americans as died on 9/11—every four days. The Covid-19 pandemic, the long-term threat to US infrastructure from climate and weather changes, and the increasing non-kinetic actions by nation-state adversaries in 2020 that seek to undermine US power, 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.

**Endnotes**


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.
CHAIRMAN
*John F.W. Rogers
EXECUTIVE CHAIRMAN
*James L. Jones
EMERITUS
CHAIRMAN EMERITUS
*James L. Jones
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. Lodal
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
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim
Olin Wethington
Maciej Witucki
Neal S. Wolin
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