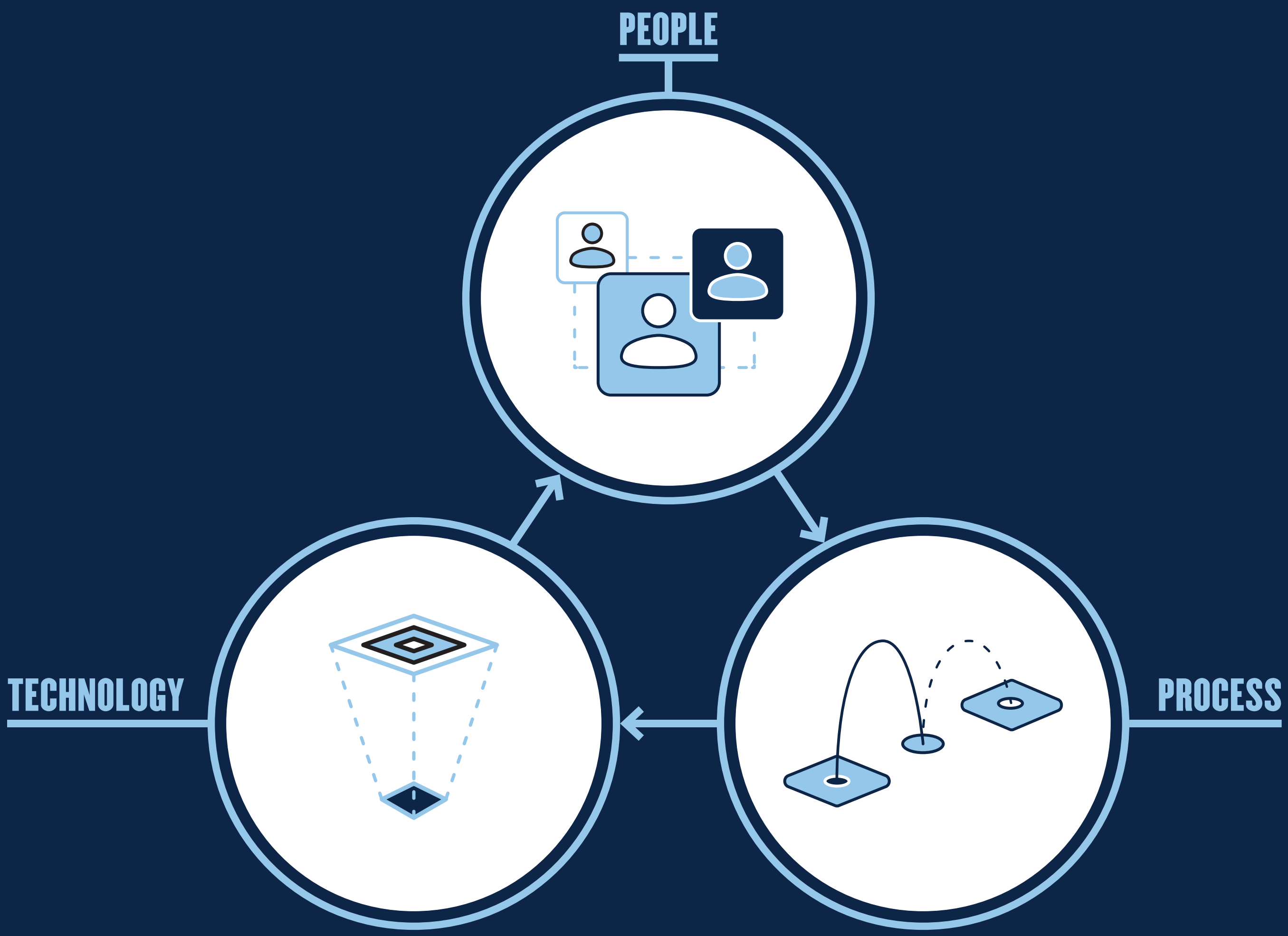
JUNE 2020

ANTICIPATING AND ADDRESSING THE CHALLENGES FACING THE HOMELAND SECURITY ENTERPRISE IN THE COMING DECADE

20 / 20 PROJECT ON THE STATE OF THE HOMELAND SECURITY ENTERPRISE



Grant Thornton

Homeland Security & Defense
Business Council

Contents

KEY TERMS FOUND IN THE 20/20 PROJECT REPORT:

↳ **Homeland Security Enterprise (HSE):** The entities—comprised of federal agencies (including, but not limited to, Department of Homeland Security [DHS], Department of Defense [DoD], Department of Justice [DoJ], Department of Energy, State Department, Health and Human Services and the Intelligence Community), state and local government agencies, global partners, academia, civil society, and private sector companies—that work together to accomplish the homeland security mission.

↳ **Homeland Security Industrial Base (HSIB):** The private sector companies that provide the technology, services, and product solutions essential to support the HSE and the homeland security mission.

THE 20/20 PROJECT ON THE STATE OF THE HOMELAND SECURITY ENTERPRISE

The 20/20 Project on the State of the Homeland Security Enterprise is a five-year initiative of the Homeland Security & Defense Business Council (HSDBC), in partnership with our member and pro bono project manager, Grant Thornton Public Sector LLP. The Project collects perspectives, experiences, and recommendations of experts. Current and former government officials and industry executives across the homeland security enterprise (HSE) have contributed to the Project through annual surveys, one-on-one interviews, focus groups, and the Council's ***National Conversations.***

The Project embraces the concept of 20/20 "clarity of vision." The Project gathers insights and recommendations from experts in government and industry regarding the challenges that affect the relationship between the two sectors and the delivery of service, product, and technology solutions to the homeland security mission. It serves as a source of information, education, best practices, lessons learned, and suggested actions to help the HSE continue to mature and provide the highest level of security for our nation in alignment with the commemoration of the 20th anniversary of the September 11, 2001 attacks.

To preserve anonymity, we do not attribute responses or perspectives to specific individuals or provide a list of participants. Readers can download copies of this and prior reports at homelandcouncil.org/2020-project.

THE FIRST FOUR YEARS

The 20/20 Project on the State of the Homeland Security Enterprise began in 2015. It was designed as a five-year project that would conclude in 2020 as the country looked forward to a new decade. The first four editions assessed the current state of the HSE, identifying risk areas and important developments. The first report highlighted the difficulties of unifying the Department of Homeland Security (DHS) and the Unity of Effort Initiative. The second report emphasized the role of the HSE in the counterterrorism and law enforcement mission. The third report focused on the business aspect of the HSE and explored the value of the Homeland Security Industrial Base (HSIB). Last year's report, the fourth, explored the barriers to innovation and the factors within the HSE that were driving protests.

This series of reports addressed key priorities, challenges, and opportunities for maturity while providing recommendations to government and industry that would enhance operations and improve support of the mission. The reports consistently identified management-related challenges as some of the leading areas affecting the enterprise: risk aversion, staffing (including recruitment and retention), intra- and inter-agency coordination, ability to foster innovation, and effective engagement between government and industry.

Through hundreds of interviews, focus group discussions, and supporting online surveys, the first four reports tell the story of a complex enterprise and a new federal department attempting to work together to manage decentralized operations across agencies, sectors, and missions and adapt to constantly shifting threats. Many challenges are the inevitable consequence of a major government reorganization that combined multiple missions while still requiring close cooperation between agencies and with the private sector. The enterprise must react and manage risk from ever-changing threats. At the same time, it must also anticipate and adapt to new challenges in an uncertain future.

BACKGROUND OF THE PROJECT

THE FINAL REPORT

The fifth and final year of the ***20/20 Project*** shifts focus from current operations to the future of the enterprise. The data on which the report is based stems from a series of focus group interviews and online surveys. It captures a broad range of perspectives and insights from industry professionals, government officials, and academic experts working closely within the enterprise. The report examines the needs and challenges confronting the HSE over the next decade across three core areas—**people, process, and technology**—as the enterprise copes with a rapidly changing mission environment. The report offers a strategic look at the future homeland security environment, the capabilities needed to respond to that environment, the barriers to acquiring those capabilities, and possible solutions or recommendations for overcoming them. The report provides a framework designed to help the entire enterprise work together and take action.

Interviews for this year's final report were conducted during the summer and early fall of 2019—well before the appearance of the COVID-19 pandemic and the nation-wide demonstrations following the death of George Floyd. Therefore, the report's insights and analysis do not reflect the enterprise's response to these unprecedented, ongoing challenges. Nevertheless, the report identifies a number of factors that have affected the enterprise's ability to cope with an emerging threat and will likely affect how effectively the enterprise is able to anticipate and adapt to future challenges.

EXECUTIVE SUMMARY

In the fall of 2019, we engaged hundreds of current and former government officials, private sector leaders, and academic representatives in both an online survey as well as a series of focus groups to discuss the needs and challenges confronting the homeland security enterprise over the next decade. Focus groups were conducted in two parts. First, the participants identified current trends and emerging issues that would have substantial implications to the future mission environment. Then, the participants explored what the enterprise would need through the lenses of three capabilities—**people, process, and technology**—to respond effectively in that environment, the barriers to acquiring those capabilities, and possible solutions or recommendations for overcoming them.

The following trends and factors were identified as key drivers of the future homeland security environment:

- **Increasing and rapidly evolving threats—**In a threat environment that is vast and uncertain, the enterprise will require a workforce with a wide range of skills, experience, and knowledge and agile business processes that allow for informed decision-making.
- **Speed and impact of technological change—**The pace of technological change and the growing importance of artificial intelligence, robotics, automation, and new software tools such as blockchain, along with emerging technologies such as 5G and quantum computing, will affect virtually every aspect of the future homeland security mission environment. These technologies will transform industries and infrastructures, enhance innovation and efficiency, create new security threats, and change the global workforce.
- **Changing population and workforce—**The changing demographics and increased diversity of the US population, along with new business practices and generational changes in the workforce, will create several human capital challenges over the next decade.
- **Politicization of the homeland security mission—**American politics has become increasingly polarized in ways that affect many parts of the homeland security mission including law enforcement functions, immigration and border security, and disaster preparedness. These issues will impact the ability to recruit and maintain the workforce and support needed to run a complex multi-mission organization and to form needed public-private partnerships.

The report explains these trends in more depth and each chapter describes the challenges and expected impact to people, process, and technology as well as opportunities for action around each of these capabilities. Participants agreed that the enterprise's ability to operate effectively in the future environment will rest largely on a few key issues, mainly the ability to:

- **Reform the hiring and security clearance process,**
- **Attract and retain cyber and technical talent,**
- **Increase the speed and flexibility of business processes and informed decision-making,**
- **Enable greater mobility between the public and private sectors,**
- **Shift to a culture of effective risk management and innovative problem solving,**
- **Adopt emerging technologies; and**
- **Improve the public's awareness and perception of the homeland security mission**

To address these issues, the final recommendations section sets forth four collective actions that would not require legislation but if implemented, would allow government, industry, and academia to work together to respond to whatever challenges present in the next decade. These include:

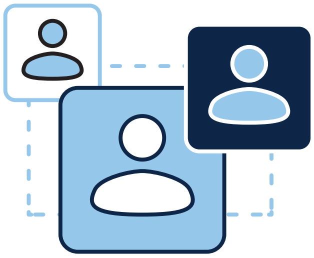
- **Strengthening mechanisms that establish and implement a national-level unifying vision for coordinated homeland security policy, strategy, planning, and operations;**
- **Providing a venue for assessing future homeland security mission challenges and related people, process, and technology capabilities that brings together the expertise and perspectives from across the enterprise;**
- **Enhancing homeland security professional development through existing and new programs to promote mobility and sharing of expertise across agencies and sectors; and**
- **Increasing the speed of business processes and informed decision-making through business process innovation groups**

INTRODUCTION

The fifth and final year of the ***20/20 Project*** considers the critical problem of ***"Anticipating and Addressing the Challenges Facing the Homeland Security Enterprise in the Coming Decade."*** Through an online survey and series of focus group discussions with subject matter experts drawn from all sectors, the project sought to understand the evolving nature of future homeland security mission challenges and what each sector—**government, industry, and academia**—must do to overcome obstacles and seize opportunities as they work together to develop, acquire, and implement needed capabilities.

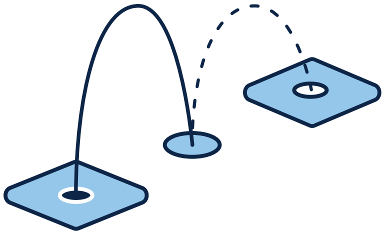
Drawing on the survey results (presented in the appendix to this report), focus group participants were asked to identify trends, factors, and mission challenges that would shape the future homeland security environment over the next ten years. Participants also analyzed the capabilities that the enterprise will need to operate effectively in that environment and discussed the obstacles and opportunities associated with trying to build and acquire those capabilities. The report summarizes key findings from the discussions and the recommendations from participants as to what each sector of the enterprise must do, both individually and collectively, to meet the needs of the future.

Participants discussed capabilities across three topic areas: **PEOPLE, PROCESS, AND TECHNOLOGY.**



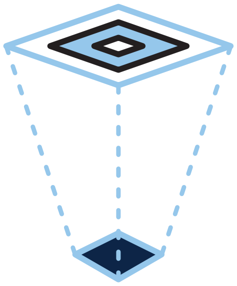
PEOPLE

The talents, skills, knowledge, and training needed to anticipate and address the homeland security mission challenges of the next decade.



PROCESS

The strategic, leadership, operational, and management processes needed to enable the sectors to work together to anticipate and address the mission challenges of the next decade.



TECHNOLOGY

The technologies and other material tools needed to address the mission challenges of the next decade.

SECTION I:

FUTURE HOMELAND SECURITY ENVIRONMENT

Rather than try to predict the likelihood of a specific event occurring in an uncertain future, focus group participants identified current **trends and emerging issues** that would have substantial implications to the future mission environment. This section describes the factors that will drive the future environment and the anticipated impact to the homeland security mission.

TRENDS

INCREASING AND EVOLVING THREATS AND RISKS

The United States is expected to face an increase in both man-made and natural threats over the next decade (and beyond) that could affect the physical and economic security of the nation. The threat of terrorism will continue from certain domestic groups as well as non-state and nation-state adversaries. Threats to soft targets will persist, as will the possibility that terrorists can acquire sophisticated and powerful biological, radiological, or chemical weapons. Terrorists, criminals, and nation states are expected to resort to cyberattacks, using new techniques that exploit vulnerabilities in emerging technologies and blur the boundaries between physical and cyber risks. Climate change and global demographic, political, and economic trends will bring increased pressures on infrastructures, food production, and access to clean water—as well as prompt large migrant and refugee flows. Natural disasters—including catastrophic earthquakes and mega-storms—and global health crises such as pandemics could increase and strike without much advance warning. To plan for and respond to these increasing and evolving threats, the enterprise will require a workforce with a wide range of skills, experience, and knowledge. It will require quick and agile procurement processes to acquire the products, technologies, and services needed to respond to specific threats and changing priorities. The enterprise must focus on building flexibility, scalability, and greater efficiency into all aspects of planning, policymaking, and business processes.

SPEED AND IMPACT OF TECHNOLOGICAL CHANGE

> **"There seems to be more focus on 'first to market' than on learning the lessons of the past. Focus is on short-term gains rather than planning for the future."**
>
> **– Academic Expert**

The pace of technological change and the growing use of artificial intelligence, robotics, automation, and blockchain, along with emerging technologies such as 5G and quantum computing, will affect virtually every aspect of the future homeland security mission environment. These technologies are expected to transform entire industries and infrastructures, enhance innovation and efficiency, and change the global workforce. Emerging technologies will also have profound impact on security threats and opportunities. New technologies will create security vulnerabilities that adversaries can exploit. If properly implemented, these technological solutions can also produce powerful new security capabilities or increase the resilience of critical functions, assets, and networks. Technological change will also change the skills needed by the future workforce and have a dramatic impact on how the homeland security mission is executed. Some jobs that exist today will not exist tomorrow, while requirements for new skills will emerge. The enterprise will have to juggle taking advantage of the security benefits offered by these new technologies while minimizing new risks and unintended consequences. Business and organizational processes across the federal government, particularly at DHS, and throughout industry (e.g., hiring, training, acquisition and procurement, policy-making, law making, personnel security, operations and strategy) will need to reflect the same speed, flexibility, efficiency, and desire for innovation. This will require a culture shift to risk taking and management as well as a culture of solving problems and encouraging new ideas.

Technological change is also driving the increasing importance of data in all aspects of life—economic and financial activities, infrastructure and industrial operations, domestic and global communications, politics, and all areas of national and homeland security. Due to the ubiquitous and growing use of the internet, social media, the internet of things, and internet-based control and communications systems, virtually every personal and operational interaction in society generates and depends on data. The availability of data presents significant opportunities for more effective problem solving and decision-making, more efficient business transactions, and the earlier recognition of emerging threats and risks. At the same time, bad actors can manipulate or misuse data in ways that threaten national security, the political process, economic and financial interests, individual privacy, and undermine confidence in government. Over the next 10 years, the HSE will require increasingly sophisticated skills, tools, and processes to manage, analyze, and use data to accomplish its missions in more effective and efficient ways, while also balancing security and privacy.

CHANGING POPULATION AND WORKFORCE

The changing demographics and increased diversity of the US population, along with new business practices and generational changes in the workforce, will create several human capital issues for the HSE over the next 10 years. As many in the federal government workforce are on the verge of retirement, the generation entering the workforce expects a different work culture. They are more likely to seek a career path that involves multiple jobs, employers, and even disciplines—both out of a desire for career advancement and flexibility, and the recognition that there are fewer job opportunities in today's economy that promise long-term growth and extensive benefits. The youngest employees in today's workforce have grown up using technology. They will expect up-to-date technology and efficient processes to do their job, as well as a path for advancement. This will have enormous implications on how the HSE recruits, attracts, and retains workers.

Demographic trends also shape the homeland security mission environment. The population that the government serves and protects is more diverse than the current government workforce, which creates challenges for communication with stakeholders, public-private partnerships, and customer service focused and law enforcement operations. The ability to successfully execute any of the federal homeland security missions or the missions of the many HSE organizations across the country will require a workforce that understands what drives human behavior through the lens of different cultures, values, languages, religions, and history.

POLITICIZATION OF THE HOMELAND SECURITY MISSION

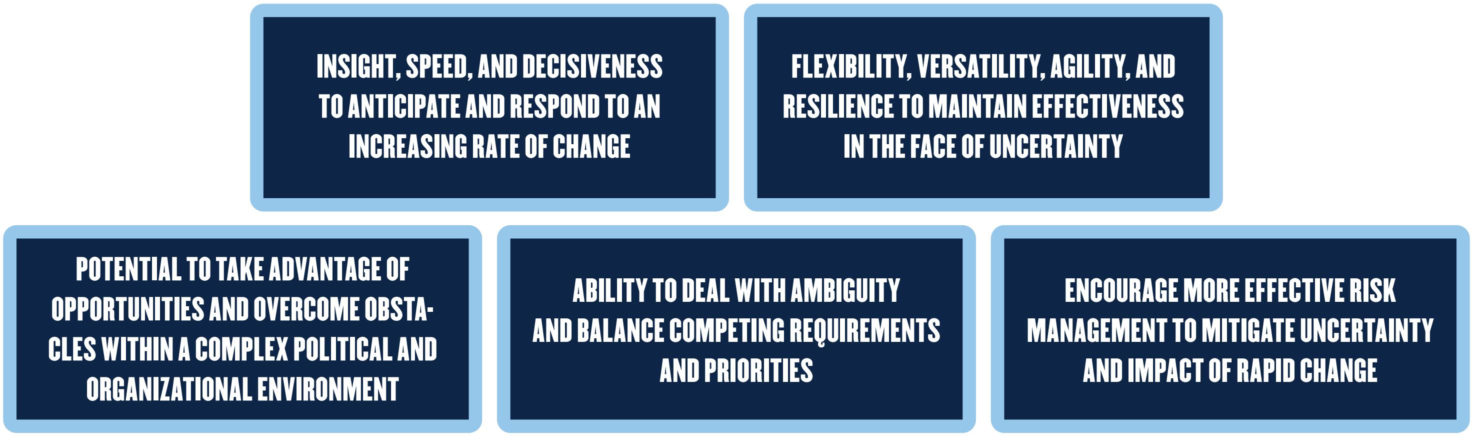
American politics have become increasingly polarized over the last several decades. That polarization affects homeland security missions involving law enforcement, immigration and border security, and disaster preparedness. Participants in our focus group discussions frequently cited politicization of the mission and public perception of the enterprise as an emerging challenge, particularly with workforce recruitment. Public perception, particularly in the wake of coverage regarding the Southwest Border and political debates over immigration enforcement, presents a challenge for the enterprise to acquire and maintain the workforce and support needed to run a complex and critical organization. Some corporations within the homeland security industrial base face pressures from their workforce to limit cooperation with homeland security agencies because of opposition to immigration enforcement and other policies. Similarly, certain local governments and law enforcement entities limit their cooperation with federal authorities out of concern for how federal immigration enforcement operations impact relations with local groups.

Participants also addressed the significant turnover and critical gaps in senior leadership across the enterprise, including senior officials in acting capacities, which hampers the ability to develop strategy and coordinate policies and activities. As a relatively new entity, the enterprise is at a critical juncture to mature processes and operations. That requires strong leadership. Similar concerns undermine the ability of the enterprise to carry out critical disaster response operations and infrastructure resilience planning. The public perception of enterprise, to which our participants applied no judgment, reduces its ability to form necessary public-private partnerships. Politicization and leadership turmoil can negatively affect workforce morale and inhibit the ability to attract and retain talent. These challenges could erode the working relationships among the three sectors of the enterprise by undercutting shared commitment to and understanding of mission priorities.

SECTION II:

CAPABILITIES

The trends described in the previous section impact each of the three capability areas—**people, process, and technology**—required by the enterprise to prepare for and respond to the challenges and opportunities of the future. All three capability areas are interconnected, and the enterprise must integrate improvements in each to create an operating system that is effective, fast, versatile, scalable, agile, efficient, and resilient. The enterprise must have the following characteristics:



INSIGHT, SPEED, AND DECISIVENESS TO ANTICIPATE AND RESPOND TO AN INCREASING RATE OF CHANGE

FLEXIBILITY, VERSATILITY, AGILITY, AND RESILIENCE TO MAINTAIN EFFECTIVENESS IN THE FACE OF UNCERTAINTY

POTENTIAL TO TAKE ADVANTAGE OF OPPORTUNITIES AND OVERCOME OBSTACLES WITHIN A COMPLEX POLITICAL AND ORGANIZATIONAL ENVIRONMENT

ABILITY TO DEAL WITH AMBIGUITY AND BALANCE COMPETING REQUIREMENTS AND PRIORITIES

ENCOURAGE MORE EFFECTIVE RISK MANAGEMENT TO MITIGATE UNCERTAINTY AND IMPACT OF RAPID CHANGE

↳ Figure 1: Essential Characteristics of Future Capabilities

These traits must be inherent in leadership perspectives, business models, and professional approaches to every task. It is particularly important that the enterprise embrace more open and effective risk management and informed risk taking at all levels—strategic, operational, and management. Leaders, managers, and staff throughout the enterprise must do everything possible to anticipate future threats and requirements and plan accordingly. At the same time, they must cope with uncertainty and the need for timely responses to unforeseen challenges, which requires a willingness to accept reasonable risks, "failing forward" when necessary, and achieving desired outcomes more quickly.

PEOPLE

Survey respondents and focus group participants identified people as the central capability for executing the homeland security mission across all three sectors of the enterprise. The government workforce must be able to develop appropriate strategies, policies, and plans to carry out effective protection, enforcement, response operations, and management functions. Industry brings workers with the skills to develop and provide the combination of technologies, products, and service solutions required by government to fulfill its mission. Academia provides scholars who conduct research, develop teaching curricula, and educate the future homeland security workforce.

NEEDS AND REQUIREMENTS

Due to the nature and scope of evolving and uncertain threats the HSE may face in the future, the enterprise needs workers with foresight based on operational and technical expertise as well as experience and insights from across multiple disciplines. The ability to cross-train and move within and between sectors will be essential. The HSE will need to shift the culture of effective risk management to encourage new ideas, learn quickly from failures, and solve challenging problems. This will require a government workforce that thinks differently, guided by senior leadership that embraces risk and encourages engagement with industry to address mission-critical problems. Industry will need workers with analytical skills to provide operational support and to apply creative management approaches and emerging technologies to emerging problems.

All participants agreed that the HSE will continue to require a professional workforce with expertise in multiple disciplines, including mission operations; organizational, financial, and acquisition management; and information and other technologies. Homeland security missions are inherently complex and are changing rapidly. The sectors must work together to develop the necessary skills and train the current and future workforce to carry out these missions. Likewise, the enterprise must develop and apply the management talents necessary to cope effectively with uncertainty and complexity. All sectors of the HSE must also attract and retain workers with digital literacy, computer science knowledge, and an understanding of how physical and cyber security converge. Workers will also need strong analytical skills to effectively manage increasing amounts of data and to translate that data into actionable information for leadership, operators, and external stakeholders. As government tries to increase its speed to adopt new technologies, it will need to build a strong acquisition workforce with the technical knowledge to accurately define requirements and to understand what it is evaluating.

> **"There needs to be an increase in funding for academic STEM homeland security programs…focusing on thought leadership, T&D, innovation, and new technologies."**
>
> **– Industry Executive/Private Sector Employee**

Because of changing workforce demographics, future leaders must have the ability to manage a multi-generational workforce and understand a younger generation that desires greater job mobility. As the population that the government serves grows more diverse, employers within the HSE will need to place greater emphasis on attracting workers with knowledge and appreciation of different cultures, values, languages, and religions.

CONCEPTUAL SKILLS

- **Ability to manage acceptable risk**
- **Ability to think critically and analyze complex problems**
- **Ability to think about the unknown**
- **Ability to think "outside the box"**
- **Ability to think strategically**
- **Ability to manage a dynamic and multi-generational workforce**
- **Ability to communicate complex technical and policy issues**
- **Ability to integrate and coordinate across mission areas and between the public and private sectors**

EXPERTISE & KNOWLEDGE

- **Homeland security mission expertise and ability to conduct operations**
- **STEM and computer science**
- **Digital literacy**
- **Technical expertise to understand future application of technology and knowledge of emerging threats**
- **Understanding of homeland security policy environment through history and political science**
- **Understanding of different cultures, languages, religions, and values**
- **Appreciation for relationship between physical and cyber security**

EXPERIENCE & TRAINING

- **Experience conducting complex homeland security operations involving multiple agencies and sectors**
- **Public relations and marketing experience**
- **Acquisition and procurement**
- **Training to build leaders with diverse thoughts**
- **Training to build the skills of senior leaders**
- **Training on how to manage risk**

↳ **Fig. 2**

Figure 2: Homeland Security Workforce of the Future describes the range of skills, knowledge, experience, and training identified by survey respondents and focus group participants necessary to build a workforce that can respond to the future homeland security environment

OBSTACLES AND BARRIERS

Focus group participants identified the top barriers that impede the ability of both the public and private sector to acquire the workforce of the future.

Competition for Cyber and Technical Talent

There is considerable competition across the government and private sector for workers with cyber and technical skills. Focus group participants noted an already existing shortage of workers with these skills along with increasing future demand across law enforcement and intelligence agencies, as well as the private sector. DHS and the HSE as a whole may have more difficulty in attracting and retaining future workers with these skills than other parts of government or industry sectors. The private sector, including federal contracting companies, often has the advantage of higher wages, which can be more attractive to job candidates. Individuals, who may otherwise have an interest in homeland security, or in joining DHS for the importance of the mission, may decide it is too controversial or find better opportunities at intelligence or defense organizations. Highly publicized morale problems at DHS over the past several years also make other federal agencies more attractive career choices. These factors are likely to contribute to the growing shortage of workers across the HSE. Finding ways for the public and private sectors to work together to increase the pipeline of talent is critical to building the future workforce.

Participants also discussed competition within certain disciplines that are important to the homeland security mission, such as law enforcement opportunities at state, local, tribal, and territorial versus federal levels, or among federal agencies. This could be attributed to a lack of coordination or overriding strategy in how to position the opportunities within the enterprise or how to identify and attract potential career candidates who may come with more varied experiences than traditionally sought by the various agencies and organizations within the enterprise.

Lastly, from an academic perspective, the field of homeland security as a general research discipline is among the newest when compared to others such as defense and criminal justice. As an example, participants cited the shortage of research and funding infrastructure that may divert otherwise interested academic practitioners from entering the discipline.

Lengthy Hiring and Security Clearance Processes

The length of time and bureaucracy associated with hiring federal employees and contractors, particularly at DHS and other federal law enforcement agencies, presents one of the hardest obstacles to meeting future homeland security workforce needs. Focus group participants consistently noted the difficulties associated with obtaining security clearances and meeting agency-specific personnel security requirements (e.g., employee suitability or contractor fitness). When a job posting requires a security clearance and polygraph test, it can take one to two years for a candidate to gain the security credentials needed to begin work. Even for candidates that already have a security clearance or are currently working as a federal employee or contractor, the ability to move or perform work for another federal agency or a different component within DHS can require weeks or months of additional time for more background investigation. It is difficult to attract and retain quality talent when the hiring process is lengthy and unpredictable. Focus group participants from both government and industry shared numerous stories of having to go through the hiring process 3-4 times for a single position because candidates took other job opportunities while waiting for security investigations to conclude. This process is unsustainable in an environment with increasing threats and quickly changing priorities that may require a sudden surge in workforce hiring for response. The delays result in the loss of top talent for the HSE. Title 5 of the Code of Federal Regulations, which governs federal employment, creates a system that is slow, inflexible, and risk averse. One government survey participant summarized the problem when noting, “There is no alignment between what we want for human resources and the tools we have to achieve it.”

Lack of Job Mobility

Historically, federal employees tend to remain at the same agency for many years, sometimes devoting their entire career to one agency. Federal employment data shows that nearly one-third of the federal workforce is over the age of 55, with only eight percent of federal employees under the age of 30 (compared to the private sector where 23 percent of employees are under the age of 30). As the current federal workforce moves towards retirement after decades of service, the government is faced with a pressing need to fill those personnel gaps with new workers. However, the millennial workforce may unfavorably view federal service as requiring a long-term commitment, when they tend to seek less-restrictive job opportunities with greater options for mobility. Without changes or incentives built into the current employment system, the federal government is limited in its ability to provide job opportunities with more flexibility and mobility.

Many participants commented on the increased importance of finding workers with multi-disciplinary and cross-sector experience, but several barriers limit workers' ability to move between and across government and private sector positions as their careers develop. Once an employee leaves the federal government or stops working for a federal contracting company, they risk losing their security credentials, which leaves little flexibility for transferring valuable skills and knowledge across sectors. As noted in the previous section, the length of time involved with meeting security requirements reduces mobility and limits the ability of workers to gain and share valuable cross-sector knowledge and experience. Post-government employment restrictions add another barrier to move between government and private sector jobs. While the diverse mission sets of the enterprise make it uniquely positioned to provide employees with valuable cross-sector experiences, this cannot occur without a significant change to the hiring and security process and the enterprise-wide approach to hiring and talent management.

Politicization of the Homeland Security Mission

Politicization and lack of consensus about the homeland security mission also pose barriers to attracting, developing, and retaining the talent required across the enterprise. As a relatively new agency responsible for an as-yet poorly defined mission, DHS has not achieved the same level of public awareness as the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), or the Department of Defense. Focus group participants felt that large portions of the public would have difficulty identifying the different components that make up DHS and have limited knowledge of what they do. While many have heard of the Federal Emergency Management Agency (FEMA), participants noted its actual role is misunderstood and the public is often surprised to learn it is part of DHS. The newest DHS component, the Cybersecurity and Infrastructure Security Agency (CISA), recently changed its name from the National Protection and Programs Directorate because many, both inside and outside of the HSE, did not understand its role in cybersecurity and infrastructure protection. Many view U.S. Immigration and Customs Enforcement (ICE) negatively due to media reports and political opposition to immigration policies and enforcement actions without knowing that parts of ICE also play a critical role in stopping human trafficking and child pornography. Other parts of DHS that citizens have interacted with, such as TSA security officers or CBP officers at airports or ports of entry, are sometimes perceived as inconveniences or intrusions rather than for their mission to ensure safety and security. Media reports and political disagreements about immigration and climate change contribute to growing misconceptions about the mission and values of the HSE. Some focus group participants indicated that this creates divisiveness within the Department and leads some components to want to disassociate and separate from the agency. There are already discussions and efforts to move the Secret Service out of DHS and back to the Treasury Department. Political disagreements also affect industry activities in the HSE, as some companies feel public and employee pressure to not provide services or technologies to DHS or other government components.

DHS has spent considerable effort trying to foster a unified Department with unique missions, identities, and cultures. The recent politicization makes this already difficult task more challenging and negatively contributes to the public's perception and the reputation of the mission. To compete with other federal agencies and the private sector for top talent, participants noted the importance of the HSE working together to develop and build greater public awareness, recognition, and respect of the homeland security mission.

OPPORTUNITIES FOR ACTION

To overcome these challenges, focus group participants discussed key areas for action and recommendations for the role of government, industry, and academia.

Greater Emphasis on Explaining and Marketing the Mission

To attract and retain needed talent, the HSE must develop a unified communications strategy and enterprise-level marketing and branding efforts that explain the value and importance of the homeland security mission to the public's safety and economic security. The message must continue to offer workers both inside and out of government the chance to solve important, complex problems while protecting the security of the nation. Protecting the homeland must be seen as a valued profession requiring significant skills as well as dedication to public service—whether that service is performed within government, in the industrial base, or in academia. While so many currently working in the HSE already view the profession this way, efforts must prioritize building this perception with the general public. Leaders across the enterprise should work with education and civic organizations to present homeland security as an attractive, viable career option in schools at all levels and to youth groups.

Human capital management reforms must also reinforce the image of homeland security as a valued profession. The enterprise must focus on purpose-driven recruitment and ensure its career paths incentivize talented individuals to come to and stay with the HSE. Through thoughtful and compelling marketing and branding techniques, the HSE can acquire its future workforce by creating invested stakeholders and potential recruits who are passionate about working in homeland security.

Reform the Hiring and Security Clearance Processes

The HSE must transform the hiring process, including reforming the security clearance and personnel security processes, to ensure that individuals can start their jobs in a timely manner. Focus group participants noted there are ongoing efforts to improve the personnel security process, but improvements that actually result in speed and predictability will require strong leadership willing to push for sweeping change. Congress should also consider updating Title 5 of the Federal Code to close the gap between the federal government and private sector when it comes to hiring practices. These older laws were not designed to address today's employment needs and challenges. Reform efforts should focus on changes that increase the speed of hiring (while balancing the need to vet the workforce for security risks) and job mobility between sectors and among disciplines, allowing for more effective knowledge sharing between the public and private sectors.

Establish Exchange Programs within Government and with Industry

Government and industry should continue to explore options for exchange programs that allow employees to develop skills and experiences outside of their specific division, bureau, or agency. Within DHS, several participants cited the Loaned Executive Program as a model to consider for expansion. These programs would provide workers with the opportunity to gain cross-sector experience and would improve how sectors work together through the sharing of diverse business practices, risk management, and leadership styles. This approach would also encourage individuals to seek new career opportunities with the understanding that they are not restricted from returning to a previous post.

One focus group participant emphasized the often-overlooked opportunity for the federal government to attract and retain younger workers, saying, "The federal government, and especially the homeland security field, has ample opportunity for young people who want to do a job for a few months or years and then move on to something else. The government is a big place, and we need to start thinking like that in order to retain young talent." By leveraging options such as flexible work arrangements, details, Intergovernmental Personnel Act (IPA) agreements, and exchange or fellowship programs, the HSE can increase retention, share talent and best practices, and reduce attrition.

The Digital Services model was cited as an opportunity for private sector employees with specific technical expertise to bring their skills to the federal government for two to four years to solve a problem before moving on to other opportunities. This method not only facilitates the movement of private sector talent into the federal government, but also encourages exploration of public sector opportunities not considered previously. These types of employment models should take on greater importance within the HSE over the next decade in order to meet the needs of the future workforce.

Collaborate with Academia to Inform the Educational Curriculum

Both government and industry must work with institutions of higher education, especially those offering specialized homeland security programs, to inform educational curricula and create a pipeline of graduates with the knowledge, skills, and abilities needed by the HSE. Academia must focus on molding students into futurist thinkers, risk-takers, and problem-solvers. While there has been greater emphasis in recent years on building STEM skills, more efforts are needed to develop technical skills in conjunction with the humanities, as both will play a strong role in the future of the HSE workforce.

Senior leadership development will play a critical role in changing a culture of risk aversion into one of effective risk management. Training opportunities are needed to ensure leaders take a forward-looking approach to anticipate and meet new challenges. One focus group participant questioned whether there was a need to create a homeland security version of the Department of Defense's senior service colleges to promote professional development of leaders involved in homeland strategy, planning, operations, and management. While some variations of this exist at a small scale (such as the Center for Homeland Defense and Security at the Naval Postgraduate School), greater efforts are needed between government, industry, and academia to coordinate the approach to educating the future workforce.

↳ **KEY TAKEAWAYS**

FUTURE CAPABILITIES

- Workers with specialized, technical expertise
- Opportunities to cross-train and have job mobility
- Effective risk management

OBSTACLES/BARRIERS

- Increasing competition for cyber and technical talent
- Lengthy hiring process
- Lack of mobility
- Politicization and confusion of the mission

OPPORTUNITIES

- Increase focus on marketing and branding
- Reform the hiring and security clearance processes
- Establish exchange programs between government and industry
- Collaborate with academia to inform educationa curricula

PROCESS

Meeting the challenges of the future homeland security mission environment requires foresight, flexibility, and agility. As HSE human capital and technological capabilities rapidly evolve, so must the mission, operational, and management processes they depend on. This section examines the strategic, operational, and managerial processes needed to enable the sectors within the HSE to work together to anticipate and address a changing mission environment.

NEEDS AND REQUIREMENTS

The HSE requires processes that support unity and collaboration among all three sectors, guided by a shared strategic vision and carrying out operations that maximize coordination while minimizing duplication. The elimination of organizational, cultural, and procedural silos and barriers within agencies, between agencies, and between agencies and the private sector will demand leadership and organizational commitment to open and transparent processes and greater capacity to address complex security challenges and manage risk through cooperative effort.

> **"Government needs better coordination mechanisms with industry and infrastructure sectors. Supply chains and relationship networks are too complex...We need less talk and more action."**
>
> **– Current Government Official**

As cited by participants, silos are broken down through a shared strategic vision that encourages collaboration among government agencies and with industry and academia. By sharing a strategic view of the homeland security mission and its objectives, the HSE can more closely connect mission requirements to current and future capability needs. In turn, this will enable more effective collaboration among sectors as each develops and applies its people/process/technology capabilities against shared problems. Creating a shared strategic vision requires assessment and planning processes that can anticipate future threats and mission environments—or at a minimum inform risk management calculations in the face of uncertainty. While such efforts are largely the province of government leaders and planning staffs, other contributors in academia and industry can also have an important role to play. Academics help identify and assess future technological, social, economic, and political trends, while establishing a conceptual foundation for addressing them. Industry, which drives many of those trends, can also contribute a view of the future, particularly how emerging technologies may affect future risks and capabilities.

Similar forward-looking processes are needed at the operational and managerial levels. The Defense establishment expends huge efforts to conceptualize, develop, test, and deploy operational procedures and doctrines to ensure that its forces can make the most effective use of highly trained personnel and emerging technical capabilities. At its core, the HSE is also an operational entity, and needs to devote an appropriate level of analytical and staff resources to finding ways to more effectively execute its homeland security missions. Again, academia and industry can also contribute positively.

> **"All organizations need to recognize that they have a role in contributing to the nation's resilience by develop[ing] business continuity/emergency operations plans."**
>
> **– Academic Expert**

Management reforms are also needed to improve efficiency and effectiveness. The HSE must facilitate access to talent and implement streamlined, efficient hiring and clearance processes in order to ensure that the right personnel can be recruited and retained to support the HSE mission. Better hiring and acquisition processes are required so government can obtain—and industry can provide—the people, services, and technological capabilities needed to meet changing mission requirements. Needed changes range from a clearance process that allows for freer movement of personnel across the enterprise, to additional innovation in shared services and procurements involving multiple levels of government. Tasked with facing evolving threats, timely access to appropriate people and technologies directly relates to mission effectiveness and allows government agencies to be more responsive to change in their operating environment. This also allows greater control over resource management.

One of the more innovation-focused small-group discussions explored how the HSE could encourage leaders to cope with uncertainties. Participants acknowledged that because some problems require multidisciplinary approaches, the HSE at all levels should explore iterative and collaborative processes to address the threats of the future. For example, the processes for creating counter-intelligence tools and solutions to combat decentralized terror networks could employ an agile process methodology. The complexity of the issues facing the HSE—including climate change, natural disasters, distributed cyber threats, and technological change—requires rapid, astute approaches to development that exceed the speed of threats.

The future of the HSE is characterized by rapid advances in technology in response to the threats that the nation is facing. The process of developing and deploying technology must match, and then exceed the capability of the threats, especially when it comes to human and cyber-attacks. Incorporating these cutting-edge technological advances within HSE processes, including those related to recruitment, staffing, and clearances, will play a key role in government agencies achieving their mission.

OBSTACLES AND BARRIERS

The HSE is a coalition across government, industry, and academia, each of which brings disparate processes, missions, goals, and resources. Missions often overlap among agencies, yet the agencies themselves note difficulties in communication and cooperation in achieving them. Homeland security planning and requirements development remain weak at the strategic, operational, and management levels, making it difficult to implement coordinated outcomes. Lack of protocols for information sharing and partnership development can lead to an inability to respond to new challenges and developments in a timely and well-informed manner. Further, a government acquisition process that is bureaucratic, slow, and suffers from a lack of transparency hinders necessary initiatives where the threats are rapidly evolving.

Rigid and Fragmented Processes

As noted previously, the overall homeland security mission is made up of various mission areas and is conducted by several components, spread across multiple agencies. Organizational structures, professional and cultural perspectives, and statutory requirements often drive how these various entities carry out their missions and inhibit collaboration among components and mission areas. Industry's mission-support contributions can be similarly fragmented as competitive pressures inhibit cooperation and information sharing—sometimes even within a single company. The results can undercut operational effectiveness, create redundancies and wasted efforts, and complicate definition of operational and technical requirements. This problem is exacerbated by the diffuse nature of the homeland security enterprise itself. Unlike Defense, the homeland security mission is spread over multiple agencies and includes significant responsibilities at the state and local level. Unlike the Intelligence Community, there is no "DNI" equivalent for homeland security. The dispersion of homeland security budget and oversight authority across multiple Congressional committees is a well-documented obstacle inhibiting the coordination of mission and management efforts in the Department and across the enterprise.

As noted previously, similar process obstacles influence development and deployment of effective people capabilities. Transferring between various government agencies within the HSE remains difficult, particularly with respect to the clearance process. The lack of reciprocity between agencies inhibits sharing of expertise and reinforces silos. Furthermore, the arduous clearance process is yet another factor dissuading new talent from choosing a career in government. Internally, the process is costly and time consuming, using valuable government personnel and financial resources. One participant said plainly, "We know what we want, but getting it often costs more than what we can afford in terms of staff time and focus."

This rigidity manifests in other mission support areas as well, particularly in how processes vary between legacy systems (addressed later in the Technology section) and those enabled by the history of the organization. This further reinforces organizational resistance to collaboration as agencies attempt to protect the sunk cost of legacy systems and management prerogatives.

Technology Enabled Issues for Processes

The technology used to facilitate various processes was a recurring theme in focus group discussions. The current state of technology within government is widely considered insufficient to meet contemporary challenges, resulting in inflexible processes for responding to mission needs. This also creates mission support obstacles for the HSE. Often, government agencies use obsolete technologies to conduct internal processes, such as contract closeouts, leading to delays or reduced mission readiness. This results in slower processes that cannot easily transfer among agencies and between public and private sector members of the HSE. This also reduces trust in the enterprise, a factor that focus group participants argued is critical to the mission.

OPPORTUNITIES FOR ACTION

Necessary process improvements will disrupt established patterns of behavior, challenge prerogatives and decision rights, and require regulatory and statutory changes. As one participant stated, "We must find ways to get results in less time. Bold moves are needed to shorten processes." This will require a cultural shift to more effective risk management and problem solving to enable incorporation of new ideas. The inhibitions of a complex government bureaucracy must give way to a culture of clarity and transparency. Even as compliance requirements grow in number, agencies should find ways to streamline their methods of adherence and to build new, agile processes that prepare them to meet the challenges of the next decade head on.

Improve Collaboration Across Sectors Through A Shared Strategic Vision

Improving collaboration within government components and among all sectors of the HSE requires a shared strategic and operational vision and improved resource allocations. All parts of the enterprise must share their perspectives on the requirements of the future operating environment and on what they can contribute to meeting its challenges. For its part, DHS should take the lead in describing the future homeland security mission environment and the policies, strategies, operating principles, and managerial approaches required to succeed in that environment. This future vision can then become the foundation for collaboration among government, industry, and academia as they design the capabilities that each can contribute.

Increase Strategic Alignment

Processes that incentivize and encouraged development of new operational and management approaches would increase available resources for all players in the HSE and introduce a sense of unity to the enterprise. Even within specific agencies, there exist silos between different mission groups. Shared agency-wide strategic goals are the first step in addressing internal inefficiencies. These strategic goals should be re-evaluated often to ensure buy-in from all relevant stakeholders. By improving communication and capitalizing on the mission, the HSE can develop the processes needed to enable the sectors to work together as they anticipate and address the mission challenges of the next decade.

Reform the Hiring Processes

Greater strategic alignment can lead to increased ease of talent transfer and clearance, and a renewed culture of simplicity would speak volumes to recruiting talent from, and exchanging talent with, the private sector. As detailed in other areas of this report, the operating environment of the HSE critically demands that processes for investigating and clearing personnel must be both fast and secure. The current paradigm that favors security over speed is the right choice given the balance of priorities between the two. However, the nature of the future threats facing our nation will certainly demand more in terms of speed in clearing personnel.

Adopt Emerging Technologies

The emphasis on increasing the speed of incorporating cutting-edge technology and the introduction of automation and analytics to further streamline processes would lead to greater efficiency gains within the HSE. Participants recommended that government shift the focus of much of its market research to early and emerging technologies and technological solutions. The government will not be able to acquire the technology required for the future HSE mission without a more sophisticated understanding of what emerging technologies have to offer, and how government can adopt and adapt those technologies to securely serve the HSE's mission. The government also needs a more comprehensive understanding of how technologies that are applied will affect the processes by which the HSE's mission is carried out. Industry can contribute to this effort by helping the government's mission experts understand the true capabilities and limitations of emerging technologies and helping conceptualize how those technologies will contribute to mission effectiveness.

↳ KEY TAKEAWAYS

FUTURE CAPABILITIES

- **Shared strategic vision**
- **Faster, more effective procurement processes**

OBSTACLES/BARRIERS

- **Lack of shared strategic vision**
- **Rigid and siloed processes**
- **Issues for processes enabled by technology**

FUTURE CAPABILITIES

- **Improve collaboration across sectors**
- **Strategic alignment**
- **Reform hiring processes**
- **Adoption of automation and emerging technologies**

TECHNOLOGY

Technology provides tools that can reduce risk, improve mission effectiveness, and create efficiencies throughout the HSE. Technology enables the HSE to execute a variety of functions, such as protecting and maintaining vulnerable infrastructure, improving enforcement and security operations in the field, automating routine processes, and improving the utility of data. Technology touches on both operational and mission support activities. Technology manifests across the HSE's missions in ways that we can predict, but also in ways that are yet to be realized.

NEEDS AND REQUIREMENTS

The nature of the homeland security mission and how the HSE addresses that mission are both significantly shaped by technology. Examples raised by participants included:

- Technological enhancements to advance law enforcement's ability to identify, pursue, and apprehend individuals or illicit goods coming over the borders or through ports of entry, taking security beyond physical barriers and manpower-driven solutions;
- New materials and monitoring/control devices to enhance resilience of critical infrastructures and functions;
- Next generation interoperability for first responders to enable them to respond to circumstances in a more direct manner; and
- Automation and artificial intelligence capabilities that enhance and augment how humans interact with cyber threat detection and response.

> **"Utilize both public and private sector agencies... to perform a comprehensive, nonpartisan assessment of critical infrastructure deficiencies and vulnerabilities"**
>
> **– Academic Expert**

In addition, new technologies can also pose unintended consequences in the form of new threats or undermined security. In considering the impact of technology on the homeland security mission, all three sectors of the enterprise must examine two questions: How can advancing technologies contribute to mission and operational effectiveness? Moreover, what challenges and risks do new technologies pose? This requires a shared vision of future mission challenges, as well as an understanding of operational and management requirements and the potential consequences of technological innovations.

Technological change affects virtually every aspect of the homeland security environment. New technology will bring more effective capabilities to mission-critical systems and processes that are at the core of the HSE, including traditional human-driven aspects of security, protection, and enforcement operations as well as software-driven aspects of security such as digital surveillance and screening. New technology will also improve the effectiveness of homeland security operations across broad mission areas, including border security and disaster relief, and will contribute to the security of critical infrastructure. Emerging technologies such as software-defined networks, autonomous systems, and advanced materials and manufacturing technologies are transforming critical infrastructures and functions, providing both significant security and resilience opportunities and risks. In terms of business operations, new technology will improve the efficiency and effectiveness of management systems to provide better service to internal data users and external stakeholders. Though this will demand more agile and flexible digital environments that are able to overcome the challenges and barriers currently affecting the HSE, it is possible to use technology as a tool to transform the enterprise.

While the HSE is well positioned to reap the benefits of technology, government officials and industry leaders often feel constrained by challenges that make it difficult to fully realize technology's potential benefits or avoid the pitfalls. Because of the speed and scope of technological developments, it is hard for any of the three sectors to anticipate how those advances will affect the future security, economic, and social environments—for good and bad. When trying to apply new technologies to mission and mission-support requirements, complex approval and development processes, limited resources, archaic or nonexistent infrastructure, and insufficient talent can slow the adoption of new technology and curb progress towards modernization. These challenges and barriers, however, are not insurmountable. Lessons from successful organizations that have led the adoption of technological transformation can improve the function of technology within the HSE and overcome the barriers associated with resource allocation, organizational culture, process improvement, and talent management.

Within the HSE, future technology has the potential to radically transform mission-critical systems and operational capabilities in ways that significantly improve mission effectiveness and meet an array of complex challenges. New technology may include physical devices such as drones, sensors, wearable technology, and robots or advanced computer software and systems like artificial intelligence, block chain, and data mining. Regardless of its form, new technology will be used to collect better data, access more complete information, develop better situational awareness, support better decision making, identify increasingly complex patterns, more securely store and access data, and give managers, operators, and analysts better tools with which to do their jobs. This will drive fundamental shifts in how the HSE works by bringing more effective technical capabilities to mission-critical systems and processes such as screening, surveillance, protection, and intelligence analysis. The following trends illustrate what the future of the HSE will need:

APPLICATION OF NEW TECHNOLOGIES TO MISSION-CRITICAL ACTIVITIES:
Emerging advancements in technology will need to be tailored to the unique and wide-ranging requirements of the HSE. New materials, innovative building techniques, smart infrastructure, and other technologies will transform the way cities and localities harden physical targets. New surveillance techniques, emerging telecommunications infrastructure, and increasing reliance on automation and digitization will have broad impacts on everything from intelligence to field operations. To better understand future needs, the HSE will require greater communication and collaboration between government and industry. Government stakeholders must articulate mission requirements and work with industry to develop and acquire new technological solutions. Industry must also bring innovative ideas to the forefront and collaborate with stakeholders to better determine how they might be applied to current and future requirements. Government, industry, and academia must work together to understand how technological changes will affect the overall homeland security mission environment and apply that understanding to future homeland security strategy. This goes well beyond identifying new operational, and management tools to support mission requirements. It also requires assessing how technological change will create new threats, enable new capabilities, and affect social, political, and economic conditions—all of which are core elements of the homeland security mission environment.

ADOPTION OF AN AGILE-BY-DESIGN APPROACH TO INNOVATION:
The development of new digital technology increasingly takes an agile-by-design approach, which uses an iterative process to develop more responsive and dynamics solutions, refining technology as it affects the organization. It will also promote transparency and quality. This approach allows for greater refinement and review of technology across its lifecycle. The iterative nature of the development process allows users to quickly identify issues and implement changes to better serve the changing needs and demands of the organization. By adopting an agile-by-design approach, the HSE will better serve its clients through rapid, feedback-driven progress.

USE OF DATA ANALYTICS AND VISUALIZATIONS:
The increased availability of data has led to an explosion in the importance of data analytics and visualizations. Data analytics can inform more effective business processes and decision-making by answering questions about what happened, why something happened, what will happen, or what should happen. Data analytics would allow the HSE to better process massive amounts of data to find innovative solutions to challenges. Using and incorporating data visualizations will also facilitate the communication of necessary information to decision-makers.

> **"Need to be able to keep up with technological changes that limit government access to information and/or provide opportunities for bad actors to exploit [vulnerabilities]."**
>
> **– Academic Expert**

Development of a Technologically Empowered Workforce:
Technology is a tool that helps the workforce tackle its most difficult problems. A workforce that can effectively use technology and communicate its functionality is critical to the successful functioning of the HSE. In the future, this will be particularly important at the leadership level, where decisions about new technology are often paired with broader strategic planning objectives and mission priorities. New technology will also have to be collaborative. Just as physical silos can inhibit

person-to-person collaboration, technological silos can interfere with even the best systems. In diverse organizations with multiple mission areas, technology will be an increasingly important linkage between operating units. Interconnectedness, particularly between and within systems, will be a crucial aspect of the new digital landscape at the HSE.

OBSTACLES AND BARRIERS

The HSE lacks an overall strategic vision for both how technology will affect the homeland security environment and how to make best use of technology to meet mission and mission support requirements. Technology risk assessments or procurement plans tend to focus on the threat posed by specific new technical capabilities or solutions to relatively narrowly defined operational or support problems. Similarly, industry focuses more on specifics as well, in response to procurements and business incentives. As noted in the process section previously, few are thinking about “the future” and its challenges, and how technology is shaping those challenges and may contribute to their solution.

Technology Silos

In discussing more immediate concerns, focus group members cited the highly compartmentalized and siloed nature of existing systems and technology. Participants noted that existing systems were designed to meet the narrow needs of single mission or function. For example, common information about foreign travelers entering the United States at domestic airports may be collected by CBP, TSA, and CIS using separate systems that were designed and built for a common purpose but maintained and managed in isolated siloes. This fractured system makes difficult to share information across operating divisions and match data from different sources within the organization. This limited ability to access cross-divisional information restricts the degree to which that information can be used to address complex or multifaceted problems. The highly compartmentalized nature of existing digital technology within the government can also make it difficult for software vendors and private industry experts to develop the type of crosscutting solutions that are often seen as benchmarks outside the federal government. As several participants noted, this not only discourages innovation, but also curbs the effectiveness of current technology and eliminates the underlying motivation for collaboration.

Ineffective Integration of Technology

Another challenge in the HSE is the deep interconnectedness between technology, people, and process. Participants repeatedly noted that technology cannot live in isolation and that people and processes must be in place to acquire, develop, customize, integrate, and maintain new digital technology. In the current environment, attracting technical experts to the HSE remains challenging, due to the current digital landscape across the government and the factors identified elsewhere in this report. Focus group participants with both prior and current government experience were almost unanimous in their assessment that the government does not have the resources, and particularly the human capital, needed to build and maintain a robust technological infrastructure. Moreover, there has been little success building a dynamic and holistic strategic plan that incorporates digital technology into the fabric of the enterprise. In the private sector, advanced digital technology, including artificial intelligence, machine learning, block chain, and cloud computing, are becoming commonplace. In government settings, these same technologies are only now being considered as alternatives to processes dominated by humans. As one participant quipped, the government is still trying to eliminate paper while the private sector is reimagining the way data are used to make decisions.

Inadequate Technical Infrastructure

The existing digital architecture used in government settings is not designed to meet the objectives of the HSE. The antiquated systems currently in use hinder the adoption and integration of more advanced technology. Participants were quick to point out that current systems, from acquisition and supply chain management to threat mitigation and data analytics, were outdated and fractured. Some participants even questioned the ability of these systems to handle the demands being placed on them. As higher-level computing and data analytics become the norm, systems that were initially designed to operate in relatively static and unchanging environments will become increasingly archaic. Thus far, the HSE has been slow to adopt cutting-edge changes needed to drive transformation and improvement in this space. Compared to the considerable evolution of the use of technology in the private sector, the government has traditionally focused on maintaining legacy systems and transitioning to a patchwork of shared services. While this approach has led to some improvements, structural barriers, including the availability, readiness, and maturity of new and existing systems, remain a challenge.

OPPORTUNITIES FOR ACTION

To develop and implement the technology needed to meet the goals of the HSE, leaders across government and the private sector will need to build, market, and adopt technological solutions that overcome the barriers discussed above.

Build a Dynamic and Responsive Technology Strategy

Meeting the challenges posed by technology will require a new way of thinking about how technology affects the homeland security mission and the HSE. Participants noted that leaders within the community need to begin to think of technology as key driver of the future mission environment, an essential tool for decision-making, and a critical resource for improving the effectiveness of operations within the enterprise. This requires building a technology strategy that can overcome near-term challenges while remaining flexible enough to address future concerns. It must also meet the functional and regulatory needs of the government, while being responsive to a diverse population of citizens and users. So-called resilient technologies that can respond to dynamic situations without failing when presented with new and unknown challenges are particularly critical in areas with complex or evolving processes. More broadly, this means shifting away from manual processes and towards increasingly automated solutions that deliver higher-value services that more directly support mission objectives and outcomes. In the private sector, artificial intelligence, cloud computing, and other technologies have been successfully integrated into the decision-making process. Similar solutions within the government sector could offer an alternative to existing legacy infrastructure and provide for greater scalability and future customization.

Integrate Technology into Existing Structures and Processes

The HSE will also need to consider how technology can be integrated into existing operational and management processes, whether applying new physical devices such as remote sensors or officer-safety systems or using new digital technology in the processing of existing information. This is closely related to the need for a more dynamic and diversified workforce that has the skill and background needed to perform these functions. Integrating technology into existing processes can be challenging if the underlying environment is not capable of supporting or maintaining those efforts. In addition to the technology itself, talent must be built for the future. Developing a systematic approach that identifies and leverages technological innovation is an essential step in developing an appropriate digital transformation strategy, but so is the development of human talent and adapting operational and management procedures to take full advantage of new technical capabilities. A dynamic and well-functioning team may require spaces that allow them to experiment with new ideas and challenges, learn from other organizations and innovators, leverage new skills, or push traditional boundaries. As one participant noted, technology is “an enabler of people,” not a direct substitute for decision-making and it is important to recognize that the human element of technology is just as important as the electrical elements.

Take a Smarter Approach to Delivery of New Technology

The rapid rate of innovation demands technology that is capable of meeting complex objectives over time. Innovative organizations have already started embedding security, privacy, and agility into their IT delivery models, transforming their technology systems into mission-centric solutions. Such approaches often rely on iterative development frameworks that emphasize delivery in stages, rather than all at once. They also rely on stakeholder engagement and collaboration across and within organizations. Many of our participants reflected on past efforts to expand technology through large-scale projects that ultimately failed because they tried to accomplish too much at once. In order to avoid those shortcomings while meeting the demands of emerging threats and challenges, leaders will need to be responsive as they develop and implement new technology.

↳ **KEY TAKEAWAYS**

FUTURE CAPABILITIES

- **Application of new technology to mission-critical activities**
- **Agile by design**
- **Data analytics and visualizations**
- **Digitally empowered workforce**

OBSTACLES/BARRIERS

- **Lack of an overall technology strategy and roadmap**
- **Technology siloes**
- **Ineffective integration of technology**
- **Lack of technical infrastructure**

FUTURE CAPABILITIES

- **Build a dynamic and responsive technology strategy**
- **Integrate technology into existing structures and processes**
- **Take a smarter approach to delivery of new technology**

SECTION III:

RECOMMENDATIONS

Much has changed in the seventeen years since the Department of Homeland Security was created. Intended to bring greater continuity to the federal government's homeland security efforts, the Department sought to strengthen the preparedness and resiliency of the nation. In that time, the Department and the broader HSE have been responsible for achieving a variety of critical missions spanning counterterrorism, economic security, cybersecurity and critical infrastructure protection, disaster preparedness, immigration, and border security.

In the coming decade, DHS and the HSE must work together to establish and operationalize a collective vision for the future that addresses the people, process, and technology requirements of the coming decade. Such a vision would help guide and inform the future development of new capabilities and tools that can more effectively respond to the wide array of future threats and challenges. This will be increasingly important as globalization and technological interconnectedness continue to accelerate. New and changing threats will continue to alter priorities, capabilities required, and technologies leveraged. As a result, the homeland security enterprise will need a diverse workforce that can think and plan for the unknown, a flexible and agile business process that supports management and operations, and an approach to emerging technologies that strengthens security and resiliency while improving the decision making process.

The challenges of the current COVID-19 pandemic response illustrate the importance of such capabilities and the dynamic nature of future challenges for the HSE. The continued safety and security of the nation will depend on the enterprise's ability to apply people, process, and technology to achieve its desired goals quickly and efficiently.

The recommendations provided below are actionable without requiring legislation. They incorporate elements of people, process, and technology to help government, industry, and academia to work together to respond to whatever challenges emerge in the decade ahead.

1 STRENGTHEN MECHANISMS TO ESTABLISH AND IMPLEMENT A NATIONAL-LEVEL UNIFYING VISION FOR COORDINATED HOMELAND SECURITY POLICY, STRATEGY, PLANNING, AND OPERATIONS

It is important to establish a coordinated all-of-government and all-of-nation vision for homeland security that can anticipate new challenges and address rapidly changing homeland security environments.

To establish and execute such a vision requires committed leadership, starting in the Executive Office of the President and extending to every other part of enterprise. The National Security Council (NSC), with its system of committees at various working levels, can provide an effective framework for policy development, implementation, and crisis management—so long as leadership remains focused and every agency with a critical role has a seat at the table. A free-standing Homeland Security Council could operate in parallel with the traditional National Security Council or remain combined with the NSC. Regardless of the leadership structure, it is essential that there is a consistent and prioritized focus on homeland security challenges; proactive efforts to drive unity and coordination within the Federal government and across all other parts of the enterprise; and clear, consistent messaging to the nation in times of crisis.

2 PROVIDE A VENUE FOR ASSESSING FUTURE HOMELAND SECURITY MISSION CHALLENGES AND RELATED PEOPLE, PROCESS, AND TECHNOLOGY CAPABILITIES THAT BRINGS TOGETHER EXPERTISE AND PERSPECTIVE FROM ACROSS THE ENTERPRISE

Government, industry, and academia must work together to understand the future of the homeland security environment and identify the capabilities that will be needed to operate effectively in that environment. DHS should therefore establish a high-level "futures office" that focuses on analytical efforts to predict and understand future threats and define future people, process, and technology requirements. Such analysis should inform the national vision for homeland security as well as policy, strategy, budget, and planning decisions. With a range of subject matter experts and technical expertise, this office would also provide critical inputs to the acquisition process and help translate mission problems into future requirements. Industry and academia could provide important insights and perspectives on the changing mission environment across sectors, the state of technology investment and long-term technology development, and better methods to foster innovation. The U.S. Army Futures Command offers some models that might be adapted to fit the needs of DHS.

The Homeland Security Advisory Council (HSAC), with modifications, could also provide insight on the future challenges of the Department. To ensure greater diversity of perspectives on the HSAC, the DHS Secretary should modify the existing HSAC charter to increase participation from private sector and academic experts. Despite the valuable role that these experts play in providing capabilities needed to fulfill the mission, both industry and academia have limited institutional voices on the HSAC. Additionally, the HSAC could consider adding a subcommittee focused solely on futures planning. This new subcommittee could work collaboratively with the existing Emerging Technologies Subcommittee and other subcommittees to provide targeted recommendations to the Secretary and senior leadership around improving business and planning processes for future threats.

3 ENHANCE HOMELAND SECURITY PROFESSIONAL DEVELOPMENT THROUGH NEW AND EXISTING PROGRAMS THAT PROMOTE DEVELOPMENT AND SHARING OF EXPERTISE AMONG PROFESSIONALS ACROSS AGENCIES AND SECTORS.

The enterprise should explore ways to increase options for workforce exchange programs that would allow mid-career employees and executives to gain valuable experience and perspectives from other disciplines and sectors. Focus group participants frequently cited the benefits of such experiences as a way of ensuring diversity of thought and building effective leadership and risk management skills. While there is considerable interest in such program today, there are limited options for this type of two-way mobility between government, industry, and academia. Within DHS, the government-wide Digital Services model, which brings needed technical expertise from the private sector to help speed the develop of digital service capabilities in government, and the Loaned Executive Program, which allows executive-level industry talent to take an unpaid appointment within DHS for up to one year, exist for limited participants. DHS has also started a pilot program called Exemplar, which details GS-11 – GS-15 employees to private, for-profit companies for training purposes in STEM fields. These programs are a great start, but additional two-way programs are needed to increase the experience and knowledge of working across sectors and disciplines. To expand the number of opportunities, non-profit organizations and industry associations like HSDBC should work together with the DHS private sector office to convene cross-sector working groups and identify ways to facilitate the design of new programs.

To address future workforce needs, the enterprise must develop a long-term strategic vision and plan to attract and grow the number of people that want to work in homeland security. The plan must also increase the technical skills and competencies of the workforce to align with the enterprise's future mission needs. This may involve greater coordination with academia to inform teaching curriculums, develop unique work opportunities for students, and show the value and importance of the homeland security mission to younger audiences (elementary, middle, and high school) through marketing campaigns. For example, programs such as the DHS Cyber Student Internship Program (CSIP) and CBP Explorers Program provide vital hands-on experience for students and mentorship from current DHS professionals. This kind of introduction to the homeland security mission and its stakeholders can increase the likelihood of students seeking long-term careers in homeland security. By broadening the spectrum of professionals in these roles to include minority serving institutions and nontraditional learners, the HSE remains in touch with the demands of serving a rapidly diversifying public while also providing important opportunities to program participants. More programs are needed to develop talent in other critical fields such as data analytics, law enforcement and justice, artificial intelligence and robotics, and emergency preparedness and response.

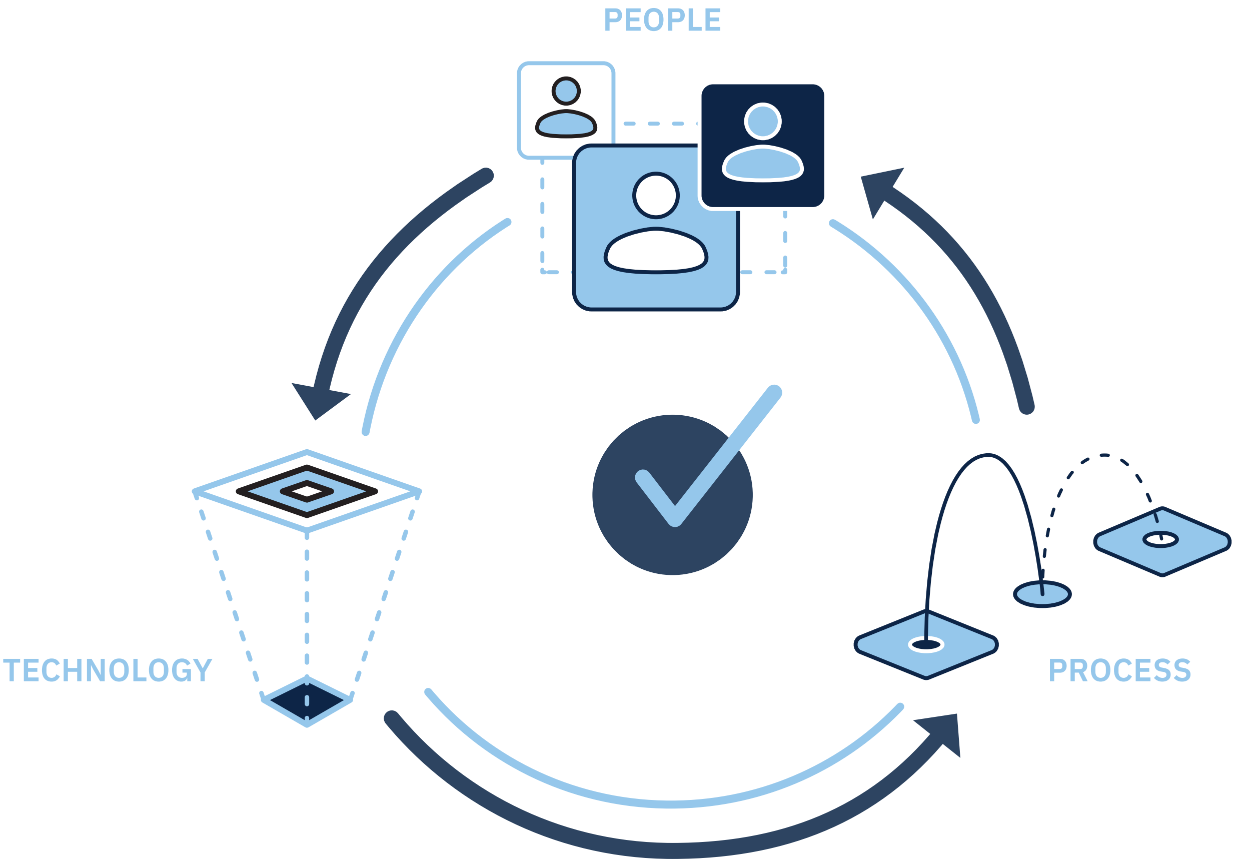
4 INCREASE THE SPEED OF BUSINESS PROCESSES AND INFORMED DECISION-MAKING THROUGH BUSINESS PROCESS INNOVATION GROUPS

As the COVID-19 pandemic illustrates, the effectiveness of any response is driven by the speed of informed decision-making and the efficiency of existing business processes. DHS should consider developing and enhancing its existing business processes using business process innovation groups that include experts from industry, academia, and government. Such initiatives could be led by an advisory council or other existing structure within the Department but should focus on shortening business processes and improving the speed of decision-making. The DHS Chief Procurement Officer has spearheaded both the creation of the DHS Procurement Innovation Lab to experiment with innovative acquisition techniques and Acquisition Innovation Roundtables (AIR) to make improvements in targeted business areas. These efforts have shown success in increasing communications with industry and encouraging measured risk taking within DHS. The AIRs have also provided a forum for government and industry to discuss ways to improve the personnel security process. More forums like these are needed and should be expanded to include workforce recruiting, training, hiring, acquisitions, personnel security, and information sharing practices.

CONCLUSION AND CALL TO ACTION

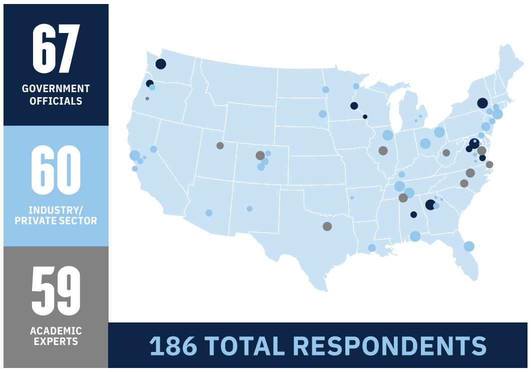
The nation faces complex homeland security challenges in an environment of rapid change and uncertainty. Anticipating and addressing these challenges will be difficult and require contributions from and collaboration by every part of the homeland security enterprise. Certain general principles must guide these efforts: a shared strategic vision; a talented homeland security workforce with deep commitment to the mission of securing the nation; agile, versatile, and effective processes at every level that can quickly achieve desired results in the face of risk and uncertainty; and the ability to develop and adopt technologies that will enhance mission capabilities while increasing security and resilience.

It is our hope that the activities of the Council and government leaders following the release of this report will continue the dialogue on how the homeland security enterprise can and must begin implementing these recommendations and taking the necessary next steps to ensure mission success over the next ten years. Such efforts can serve as a model for tackling these very same issues within the broader federal government. This is and must continue to be a joint and supportive effort among industry, academia and government. The Council is honored to serve as a facilitator and voice for industry in this effort.



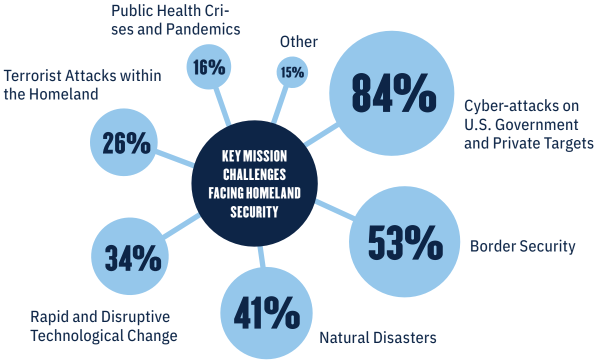
APPENDIX: SURVEY RESULTS

This year's report builds on research conducted between July and November 2019 in the form of focus groups, interviews, and an online survey. The focus group discussions were held with 82 experts including industry executives, former government leaders now in the private sector, senior government officials within the HSE, and academic leaders in the field of homeland security. The online survey collected additional information from 186 individuals.



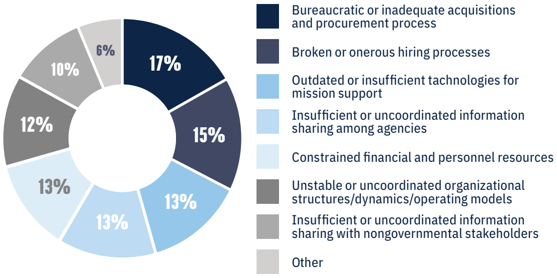
DEMOGRAPHIC PROFILE

The online survey collected information from a sample of 186 individuals with a wide-ranging demographic profile. Survey respondents varied in place of residence across the Unites States and expertise within the HSE, with 67 government officials, 60 private sector experts, and 59 academic experts participating in the survey. Respondents were asked to describe which group (government, industry, or academia) with which they primarily identified in their current work in the HSE in order to identify their background. All survey respondents, regardless of background, work in some way in the homeland security field. Of the respondents in the private sector or academia, 40 percent had previously served in a role in the HSE as a government employee or official.



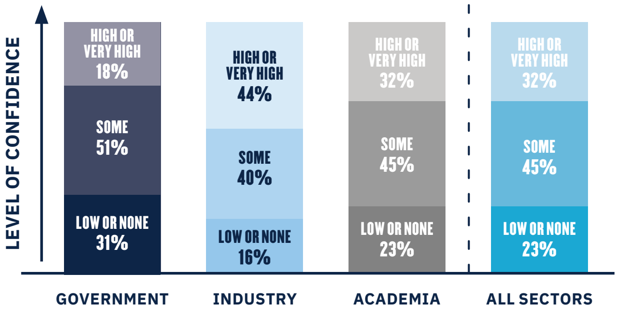
MISSION CHALLENGES

The online survey asked respondents to describe the top two to three mission challenges facing the HSE over the next decade, based on their area of expertise. Cyber-attacks on the U.S. government and private targets were identified as the highest concern, with 84 percent of respondents identifying it as a top challenge. Border security and natural disasters followed in importance, with 53 and 41 percent of respondents citing border security and natural disasters as top challenges, respectively.



MISSION SUPPORT CHALLENGES

In addition to identifying mission challenges, survey respondents were asked to describe top two or three of the most impactful mission support challenges facing the HSE over the next decade. Responses to this question were more evenly spread, with 17 percent of respondents identifying bureaucratic or inadequate acquisitions and procurement processes as a top mission challenge, and 15 percent identifying broken or onerous hiring processes as a top challenge.



CONFIDENCE

The online survey asked respondents to describe how confident they are in government's, industry's, and academia's abilities to develop and deliver core capabilities addressing homeland security challenges. Overall, about 77 percent of respondents had confidence in all sectors' ability to develop and deliver core capabilities to address homeland security challenges. Confidence was highest in industry's ability, with 44 percent of respondents describing their confidence in industry as "High or Very High," and lowest in the government's ability, with 31 percent describing their confidence in as "Low or None."

ACKNOWLEDGMENTS

The Council and Grant Thornton teams thank the hundreds of current and former homeland security government senior leaders, industry executives, subject matter experts, and academic representatives for their support and participation over the past five years of this project. We also want to acknowledge the individuals who contributed countless hours, energy, and expertise in the planning, data collection, analysis, and execution of this year's survey and report.

HSDBC MEMBER COMPANIES

Industry perspectives were provided through our focus groups and online survey. We thank the many Council member participants who represent the full range of companies that support the HSE.

AAC
ACCENTURE FEDERAL SERVICES
AKIN GUMP STRAUSS HAUER & FELD
ARDENTMC
ATTAIN
AVESHKA
BATTELLE
BAYFIRST SOLUTIONS
BOOZ ALLEN HAMILTON
CACI
CAPGEMINI
DELOITTE
DEVIS
E3 / SENTINEL
ESGI
FLATTER & ASSOCIATES, INC.
GENERAL DYNAMICS INFORMATION TECHNOLOGY
GIANT OAK
GRANT THORNTON PUBLIC SECTOR LLC
GUIDEHOUSE
IBM
INTEL FEDERAL
LEIDOS
LMI
MICROSOFT
MISSION ESSENTIAL
MITRE
NET.AMERICA
NORTHROP GRUMMAN
ORACLE
PERATON
PERSPECTA
REED TECH
SAIC
SEVATEC

PARTICIPATING GOVERNMENT OFFICIALS

This year's project once again received substantial support from high-level government officials – both current and former—representing a range of agencies from across the HSE. We especially want to thank the DHS Management Directorate and the Office of the Chief Procurement Officer for allowing the Council to use the Homeland Security Acquisition Institute to conduct the focus groups for government officials.

CBP
CISA
DHS CWMD
DHS JRC
DHS OBIM
DHS OCHCO
DHS OCPO
DHS OCSO
DHS S&T
DOE
FAA
FBI
FEMA
GSA
HHS
ICE
IRS
TREASURY
TSA
USCG
USCIS

PROJECT TEAM AND INTERVIEWERS

**GRANT THORNTON
20/20 PROJECT LEADERSHIP TEAM:**

TIM HANES, PROJECT DIRECTOR
LAUREN KIELSMEIER, PROJECT ADVISOR
VERN BUTLER, BOARD SUPPORT

COUNCIL 20/20 PROJECT TEAM:

KRISTA SWEET
JULIA TREANOR
MARC PEARL
RICK SAUNDERS, SENIOR ADVISOR

20/20 PROJECT SURVEY TEAM:

ADAM HUGHES
AMBER LUCAS
ALEX LUBOFF
KATIE SMOOTS
CHRIS MEYERS
MATTHEW SCHWARTZ
JADEN RIENDEAU
AMY NELSON
CAROLINE HICKEY
AMANDA HEJNA
MADDIE MORGAN
BEN MCBRIDE

THE 20/20 PROJECT ON THE STATE OF THE HOMELAND SECURITY ENTERPRISE SPONSOR AND PROJECT LEAD

HOMELAND SECURITY & DEFENSE BUSINESS COUNCIL
1990 M Street NW, Suite 760 – Washington DC 20036
(202) 470-6440 | www.homelandcouncil.org

The Homeland Security & Defense Business Council is a not-for-profit, non-partisan corporate membership organization comprised of the leading large, mid-tier, and small companies that support the Homeland Security Enterprise with technology, product, and service solutions. Our mission is to bring government and industry leaders together to build and strengthen relationships, increase knowledge sharing, and improve the way we conduct business together. Towards that end, our programs and initiatives focus on building better engagement models between the public and private sectors, and facilitating collaborative dialogues on the best ways to address our nation's critical homeland security issues.

GRANT THORNTON PUBLIC SECTOR LLC
1000 Wilson Blvd #1400, Arlington, VA 22209
(703) 847-7500 | www.GrantThornton.com/publicsector

Carlos Otal, National Managing Partner, Grant Thornton Public Sector LLC

Grant Thornton Public Sector LLC helps executives and managers at all levels of government maximize their performance and efficiency in the face of limited resources and increased demand for services. We give clients creative, cost-effective solutions that enhance their acquisition, financial, human capital, information technology, data analytics, and performance management. Our commitment to public sector success is burnished by a widely recognized body of thought leadership analyzing and recommending solutions to government's greatest challenges.Based in the Washington D.C. metropolitan area and a presence in over 35 cities around the country, Grant Thornton Public Sector serves federal, state, and local governments. For more information, visit grantthornton.com/publicsector.

Grant Thornton

Grant Thornton Public Sector LLC helps executives and managers at all levels of government maximize their performance and efficiency in the face of limited resources and increased demand for services. We give clients creative, cost-effective solutions that enhance their acquisition, financial, human capital, information technology, data analytics, and performance management. Our commitment to public sector success is burnished by a widely recognized body of thought leadership analyzing and recommending solutions to government's greatest challenges. Based in the Washington D.C. metropolitan area and a presence in over 35 cities around the country, Grant Thornton Public Sector serves federal, state, and local governments.

For more information, visit **grantthornton.com/publicsector.**