AFCEA Homeland Security Committee

THE IMPORTANCE OF PARTNERSHIPS TO SECURING THE HOMELAND

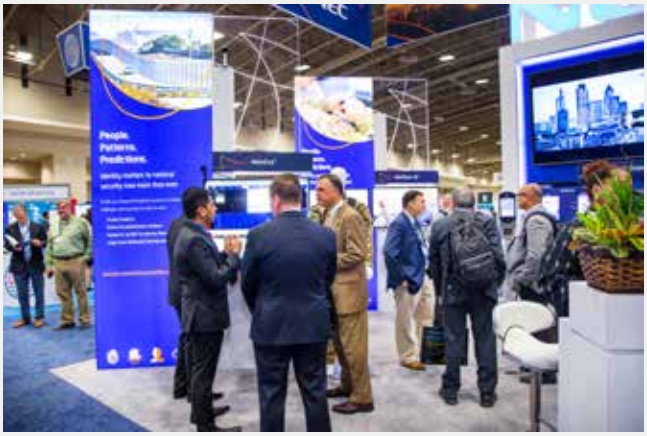
By AFCEA Homeland Security Committee

October 2017



The importance of partnerships to securing the homeland can be seen every day. One of the most widely known partnerships is the “If You See Something, Say Something™” public awareness campaign. This campaign involves federal, state, local, tribal, territorial and private-sector partners to enhance the public’s awareness of suspicious activity related to terrorism and terrorism-related crime.

PARTNERSHIPS CRITICAL TO THE FUTURE OF HOMELAND SECURITY

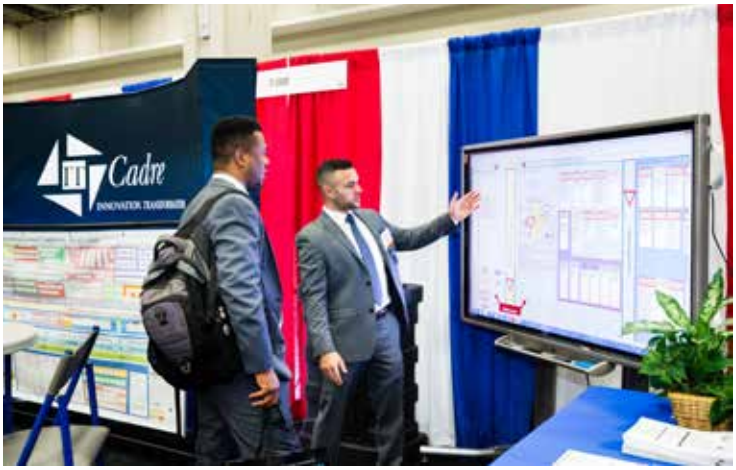


The threats to the security of our homeland are more numerous, more complex and evolving more rapidly than ever before. This accelerated threat environment is enabled in great part by technology, which has permitted threat actors to vault defensive barriers. Defeating these threats depends on forging successful public-private partnerships. Fortunately, such partnerships are increasing and present more opportunities for government and the private sector to work together.

By bringing together and leveraging the strengths of homeland security stakeholders in partnerships to achieve efficiencies and enhance technological impact, we are improving the homeland security posture. But much more work needs to be done.

PARTNERSHIPS ARE CHANGING TO ENGAGE MORE STAKEHOLDERS IN DIFFERENT WAYS

During the past few years, we've seen a proliferation of novel partnerships designed to bring all concerned parties and their resources to bear. For example, public-private sector partnerships between government, industry and academia are being nourished as part of a unity of effort initiative. All levels of government and FFRDC/lab/R&D centers, with the support of private sector partners, are sharing threat-related information and lessons learned. Information also is being shared formally and informally across agencies, regions and councils, including ISACs and ISAOs, to ensure coordination and distribution of threat-related advisories, and materials designed to safeguard critical sectors and infrastructure. For example, the FBI created its own public-private partnership called INFRAGARD and is working with state and major urban area fusion centers, along with Joint Terrorism Task Forces, to share security information and counter domestic terrorism.



DHS components are carrying out wide-ranging partnership initiatives with other government entities. U.S. Customs Border and Protection is leveraging Department of Defense equipment and lessons learned to reinforce border situational awareness and the detection of incursion events. Immigration and Customs Enforcement is collaborating with interagency government entities to integrate person-centric immigration and enforcement-related encounter data.

STILL MANY OBSTACLES TO OVERCOME

We've seen the value of partnerships in addressing threats to homeland security; however, significant roadblocks impede the vital work we're attempting to carry out to include: regulatory hurdles and policy constraints; technology gaps; political changes; and inflexible and cumbersome contracts and procurement requirements.

Despite the success in bringing innovative technology back to government, our adversaries continue to expand their cyber and physical threat capabilities exponentially. Meanwhile, the Department of Justice, FBI and state and local homeland security professionals still lack a true and integrated repository for information sharing across the homeland security spectrum. And, on a wider partnership level, improvements can still be made in information sharing, engaging nontraditional providers for innovation and providing challenge environments to evaluate industry solutions.

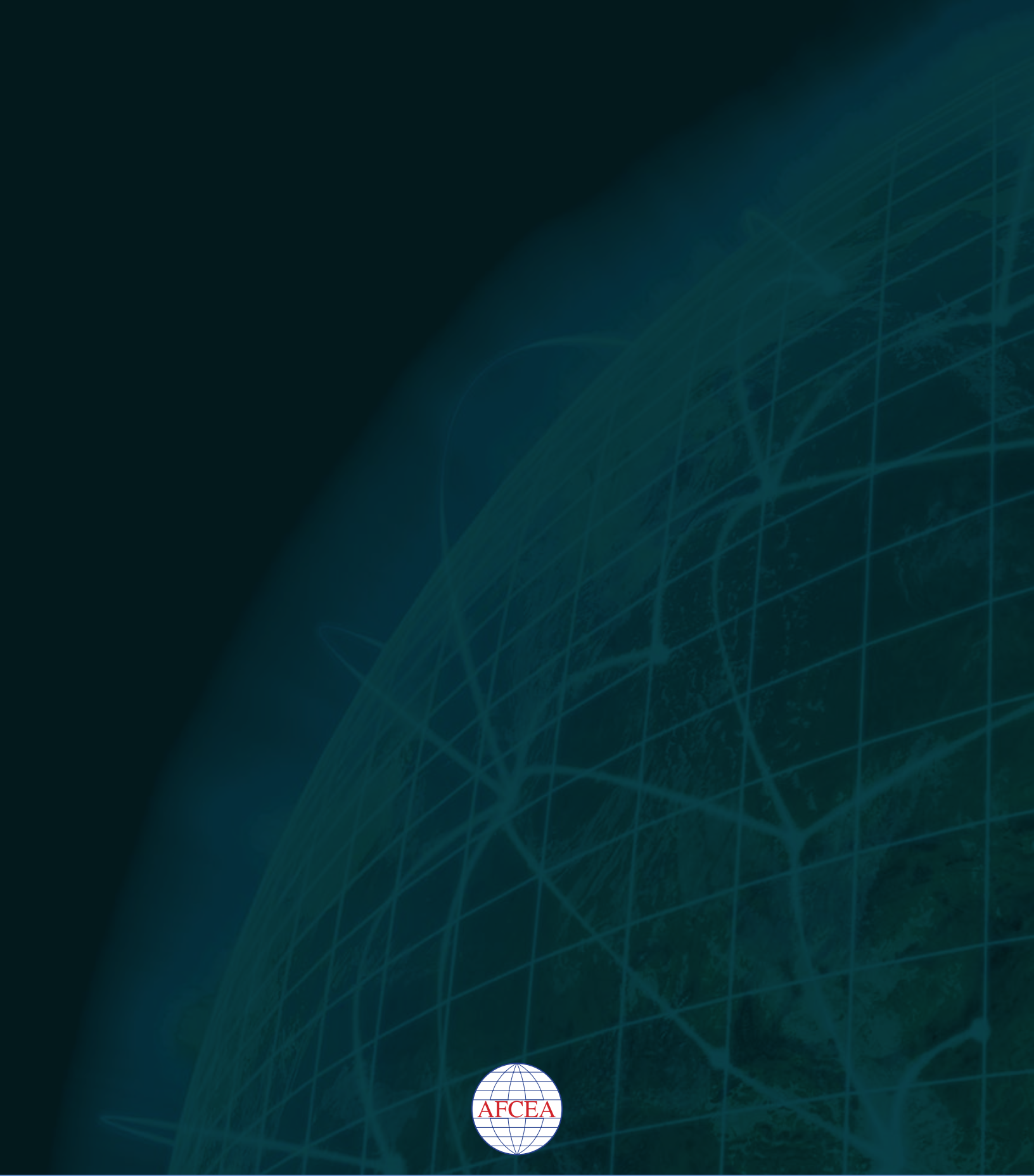
RECOMMENDATIONS FOR THE FUTURE

1. The DHS network, to include S&T and the DHS Procurement Innovation Lab, as well as various components, should increase and improve the quality of information sharing related to mission needs and acquisition/procurement opportunities. One way to reach out more broadly is to leverage existing connectors across industry and provide liaisons to existing organizations. By leveraging partners such as AFCEA, the National Defense Industrial Association, the American Council for Technology's Industry Advisory Council, the Institute of Electrical and Electronics Engineers, and the Intelligence and National Security Alliance, we can link our government and industry partners alike to create effective alliances to provide capability solutions.

2. Industry, government and academia should increase partnerships and teaming agreements across communities in mission spaces that bring together cross-industry and cross-domain stakeholders. They should engage organizations and experts who are nontraditional partners with government, placing more reliance on the public and states to look for opportunities to implement more innovation bridging like the Massachusetts Innovation Bridge, a partnership that brings together federal agencies with academia, industry and states to discover innovative ideas, products and services to enhance federal agency missions. States and industry also need to assist in shepherding these types of partnerships to contribute to the DHS mission. For example, the Applied Science Center of Innovation and Excellence in Homeland Security leverages the market influence of large businesses to help bring and fully integrate technology designed by smaller businesses into the market.

3. To address the technological gaps in the current environment, DHS organizations should continue enabling the right connections between industry and government. Through its robust network of Integrated Project Teams, DHS S&T and sponsor organizations can act as the nexus upon which partnerships between industry and challenges are established and fostered to further the DHS mission. An example of this is the MassChallenge startup accelerator program, a technology incubator that links potential technical solutions with government needs. Information sharing and analysis organizations such as the Mid-Atlantic Cyber Center bring together university, industry and government members in a state or region to share information related to cybersecurity risks and incidents. Another timely example is the national level effort of private sector companies who have teamed up with local governments in Texas to respond to the recent Hurricane Harvey recovery and response efforts.





AFCEA Homeland Security Conference White Paper

www.afcea.org/site/homelandsecurity