Building Program Awareness and Outreach

Moderator: Erik R. Pages

Presenters: Nimasheena Burns, State of North Carolina

Chris Buthe, State of California

Mike Kelleher, State of Maryland

When North Carolina began its Defense Industry Diversification Initiative (DIDI) as an OEA grantee, their motto was "if you build it, they will come," a saying that's proved true for the state so far. NC DIDI's effective outreach starts with branding, including a sleek website, derived from the Washington IR Project website, a lively social media presence, and an attractive newsletter. As NC DIDI learns what its partners find valuable, they refine their brand to reflect their partners' input. NC DIDI used graphic design software PictoChart and Canva to make nice-looking posters, and Wix to design its website, using Wix's web analytics features to track their user engagement. NC DIDI enhances its brand via partner organizations, placing their partners' logos on NC DIDI's outreach materials. This allows NC DIDI to rely on its partners' more esteemed reputation when reaching out to new organizations or organizing events (Partners can also pay for food, which helps). With their partner organizations, NC DIDI develops digestible, data-driven reports, complete with interactive web pages, that apply directly to North Carolina's various regions and industries, attracting the attention of North Carolina politicians. With the support of politicians at their meetings, NC DIDI is able to attract further partners to their organization, making sure they have a "big bat," such as the Governor, in the room for their meetings with partners.

Maryland's MEP Center, responsible for managing the state's Industry Resiliency Grant, relied on partnerships with the state Office of Military Affairs and the state Department of Commerce to develop its statewide presence. Maryland's outreach efforts revolved around its development of the Maryland Defense Directory, with their OEA efforts including a Cybersecurity Assistance Program and Defense Diversification Assistance program. Townsend University built Maryland's Defense Directory, pulling information from SAM.gov to prepopulate defense contractors. However, they had difficulty engaging companies to respond to surveys and populate or update data. The key to both cybersecurity and diversification assistance was education. By raising the level of awareness of the defense sector, companies become aware of the benefits of cybersecurity compliance and commercial diversification, where before they were satisfied with one defense contract and their current systems. Engaging with regional teams, county-level Economic Development Organizations and Chamber of Commerce luncheons are key to reaching out to businesses. However, Maryland officials advised against letting cybersecurity providers looking for sales into meetings, while partners that are helping vet and qualify cybersecurity providers should be let into the meetings. Maryland found it was most effective to piggyback off of Trade Association events to reach out to companies, then having these companies tell the story for you. Working with partners let's Maryland bring food to events or host events at Craft Breweries that proved popular.

In California, the primary provider of cybersecurity services, the CMPC MEP center, engages with every organization tangential to the IR program's efforts – including the Governor's Office, Small Business Development Centers, Procurement Technical Assistance Centers, Export Assistance Centers, Economic Development Organizations, and the Community College System. CMPC similarly partnered with

Defense Acquisition University for trainings. Their outreach is divided up: CMPC is responsible for getting people to trainings, and CASCADE (the state project) is responsible for outreach to suppliers, and workforce developers. The supply diversification sessions acted as an entry way to cybersecurity for most companies, because companies weren't interested in hearing about cyber by itself. After introducing CASCADE's business services, CMPC introduces cybersecurity. By scaring companies at this session, they become interested in learning more about cybersecurity assistance services from the CMPC. Like Maryland, cybersecurity providers are not allowed at cybersecurity assistance events, because manufacturers don't want to be sold to. While the diversification assistance events are public, the cybersecurity assistance events are private, and include folks from DoD, the MEP Centers, PTAC, and DHS to add credibility. CMPC makes it clear no recording will be made of the event and that this is an open discussion to air any problems. CMPC approaches cybersecurity as change management, where companies need to shift their culture to include cybersecurity. CMPC relates the NIST 800-171 to technical certifications companies have already undergone, such as ISO-9001, emphasizing the process requires procedural and behavioral changes in addition to technical. Framing cybersecurity compliance in terms of the company's self-interest it induces a sense of urgency. OEA grantees have the authority to induce these changes, and by keeping cyber providers trying to sell products away from businesses, OEA grantees can create the trust with businesses to build towards cyber compliance. It takes a lot of work!

Questions

How do you identify companies to reach out to?

It requires a lot of research. Finding companies and partners is a long-term investment. When reaching out to companies for cybersecurity compliance services, target companies with something to lose – a contract, reputation, technology, or the family business. SBIR/STTR recipients are motivated because they have an IP to protect and have been already advertised as recipients, making them a visible target.

How do you identify partners?

Every potential partner has value, making it easier to cooperate. Let your existing partners introduce you to their contacts and use their value to make connections. This is especially important for organizations more mature than your own with existing value. If you don't feel comfortable engaging with an organization currently, take time to evaluate their services and engage them where they provide value. Bring cybersecurity into other workshops to co-market programs others are interested in.

How do you build a board?

Your board should have values aligned with your own. Recruit board members from organizations that can pay for food. If they already have a database and partners, recruit them to the board for their listserv. Recruit partners who can get you free stuff to your board – resources, knowledge, experience, listservs, ideas, food.

Another option is creating a Technical Advisory Committee – present your work every quarter and seek their feedback/criticism. This group can evaluate how the program is going.

How do you roll out an online course? How did you decide on an online course?

In North Carolina – tried and failed with other options. Started with a cyber roadshow and developed a 50 page compliance document that was too long for companies. Identified that cyber providers were

overcharging for cyber compliance tools and so made a DFARS compliance toolkit that became a 4 hour interactive course. The course consists of an outreach, awareness and training portions, which distract from the length. Be willing to receive critical feedback and respond.

How do you develop a reputation with companies?

North Carolina's media list is 3000 publications, mostly from the Governor's Office. Local papers will report most events if you notify them. Get the Governor to the Event, and 12 tv stations will show up. They host a local show on PBS – the Situation Room. Most state agencies have their own television program. One of their pilot companies had a raid, but it became a success story when they were provided cybersecurity services. There were protests at some events – NC engaged the protestors and had them participate in panels. Engage people, even those who don't like you at first.

How do you limit service providers' sales pitches at open events?

Before arriving, have companies RSVP and sign-in, certifying their a defense contractor. Some sales companies get asked to come on behalf of their contractors. Once they pitch, they're kicked out. Once cyber providers show up, you know you're doing something right. You need to be comfortable with a small conversation. Local buy in is important – local EDO's, CoCs at the event – if they feel ownership of the project, they'll make sure the room is full.

Do you have owners of companies talk about their experience with the OEA grantee?

A lot of owners are veterans and were slow to admit they needed help in a downcycle – that's a compelling story to other companies. Everyone is afraid to talk about how they were hacked. Testimony from a community willing to share their failures and successes is very powerful. Let companies know they need to integrate cybersecurity into their culture, just like OSHA. Many areas have some form of a DoD Small Business Office. When they bring a supplier, take care of them, because the office will bring in more people and invent you to PTAC events like Navy Gold Coast (15000 people!) that let you talk to even more suppliers.

What about cybersecurity compliance for non-DoD government suppliers?

Cyber requirements are becoming necessary to get GSA, NIH and NASA contracts. The Small Business Association and Small Business Development Centers (SBDC) have a cybersecurity program. Tell them, "Do you want a lock (SBA program), or a deadbolt (DFARS/NIST 800-171)?" DFARS will become a requirement for anyone working with the electrical grid. Legislation, like California's CCPA (version of EU GDPR) is making cyber compliance a competitive advantage for companies.

For cyber compliance, how do you make sure all the right people are in the room? Might need a contract person or CEO in addition to the manager.

In California, if someone gives all the signs they want to pursue cyber compliance, CMPC asks who the company is assigning to do cybersecurity compliance as a final test. Companies generally say, "The IT Guy," which is wrong, because DFARS requires management buy-in. NIST MEP has already assigned each part of DFARS to a technical or managerial position. CMPC let's them know they need the HR Manager, CEO, Operations Manager, COO and a Champion to coordinate all portions of implementing DFARS. Its beyond the IT guy – it the company culture.

MEP tells them – we're not looking for profits, we're just trying to help the company stay profitable. They want companies to become cyber compliant. Small-medium Manufacturers don't generally have a 100% IT guy. So need to work with the small companies to help find the right people to become responsible for each DFARS item.

It's a culture change, via Digital Leadership. Not having a high level of cyber-security is a contract issue and a huge disadvantage in growing their business. This is a business problem with technical and business solutions. Relate cyber to the business' existence. MEP's help them coordinate that process. Companies don't think they'll ever be audited by the DoD – but its not the DoD auditing you, its foreign-national hackers. Bringing an FBI person to the event can help – they can simulate what its like to be hacked, which can scare companies into shape.