Q&A

Executive Viewpoint

A conversation with Alaina Clark

Assistant Director for Stakeholder Engagement, Cybersecurity and Infrastructure Security Agency

This interview continues at Carahsoft.com/innovation

How does CISA's role in the nation's cyber defense create the need for a targeted approach to working with the private sector?

As America's cyber defense agency, CISA was built on a voluntary collaboration model with our critical infrastructure partners. The vast majority of critical infrastructure is owned and operated by the private sector, so cybersecurity demands a strong public/private partnership, which we have. Frankly, I think one of the things that sets CISA apart is this voluntary model of operational collaboration.

We see ourselves as the center of gravity for bringing together the public and private sectors and helping to augment the work that the cybersecurity community is doing. Over the past 18 months, we've deepened that operational collaboration through the Joint Cyber Defense Collaborative. JCDC is comprised of like-minded organizations from the public and private sectors with a common goal of reducing risk at scale. JCDC is not CISA's alone. It's an operational forum and defense planning construct where federal agencies and critical infrastructure entities engage as co-equal partners.

Since we launched JCDC, we have been deepening the operational collaboration with industry and with our international partners. Our goal is to make cyberspace as difficult an environment as possible for our adversaries to operate in. That's where my division, the Stakeholder Engagement Division, plays an essential role. We've been charged with developing partnerships, facilitating dialogue, convening stakeholders, and promoting awareness to help CISA achieve a secure and resilient infrastructure for the American people.

We have a much more focused and robust collaboration with the public and private sectors in responding to urgent security threats. Based on these partnerships, we have also been able to develop specific resources for particular industries as needed. While we have made tremendous progress, we know there is more we can do to strengthen our collaboration.

What are the key elements of CISA's Stakeholder Engagement Strategic Plan, and how are you implementing the plan?

Because collaboration is the foundation of our success, we released a Stakeholder Engagement Strategic Plan last fall that defines areas of focus for the next three years. The plan elevates and enhances coordinated engagement in partnership activities, including the full integration of CISA's regional offices into the work that we're doing. It focuses on unifying the agency's efforts to engage and collaborate with stakeholders and partners effectively and to develop and strengthen trusted relationships.

The plan has three goals that articulate our highest priorities when working with our partners. The first goal is a commitment to collaboration. I know that's been a common theme through what I've been saying, but within the agency as well as with our stakeholders, we want to address how CISA collaboratively plans and implements stakeholder engagement and partnership activities to advance this unified mission delivery.

The second area focuses on streamlining the use of stakeholder feedback and insights to help inform the agency's offerings and

our mission delivery, with the intent of producing and delivering truly valuable products for partners.

The third area is accessibility and transparency. Through our coordinated efforts, we want to make it easy for stakeholders to quickly find and access relevant products and services, including actionable decision-support information. For example, in response to Russia's invasion of Ukraine, we created the Shields Up website so that we could share targeted, actionable cybersecurity information for a variety of partners to access and use.

What lessons have you learned along the way?

One of the biggest lessons I've learned across the span of my career — and I've worked in this voluntary partnership area for quite some time — is that when you create a new policy, initiative or resource, you need to have your partners at the table from the beginning and throughout development. You need to receive their feedback, implement their suggestions and roll out that particular program in collaboration.

Success is dependent on our partners. It's our job to ensure that they can fully utilize whatever policy or program we present to them. I have seen some of the biggest successes and also some of the biggest lessons learned based on how much we as an agency or a department not only engaged with partners, but took their feedback and implemented it. That is something I truly enjoy working with different parts of the agency on as we develop new or refined resources for partners to use.

How can agencies use CISA's resources to improve their cybersecurity posture with the help of industry?

While we recognize that we all want the absolute best cyber defenses, money can be an issue. This is especially true for state and local governments or small and medium businesses that are constrained by a limited operating budget and fewer IT staff compared to larger organizations. And cyber criminals know this. That was very apparent during the COVID-19 pandemic when we all went virtual and attackers targeted hospitals and school systems.

CISA offers a number of resources to help those smaller entities, including our cyber hygiene vulnerability scanning. It's an automated, remote scan for internet-facing systems that generates a report identifying vulnerabilities and providing mitigation recommendations to improve the cybersecurity of systems that are connected to the internet.

> "The vast majority of critical infrastructure is owned and operated by the private sector, **so cybersecurity demands a strong public/private partnership.**"

A second resource is the Cyber Security Evaluation Tool, or CSET. It's a downloadable self-assessment program that was developed by CISA, and it walks users through a comprehensive evaluation that is easy to understand and follow. One of the modules in CSET is the Ransomware Readiness Assessment, which helps organizations determine how equipped they are to defend against and recover from a ransomware incident.

The last resource I want to highlight and probably one of the most important is CISA's field staff. I can't stress enough the value that our field personnel provide. Our regional cybersecurity advisors are available on request, free of charge, and they're located across the country. They can help by doing an on-site cyber protective visit and answering any questions that partners might have. They can also walk partners through the various resources that CISA offers based on their maturity level on the cybersecurity front and can do more advanced technical assessments.

What advice do you have for other agencies on how to strengthen their partnerships with the private sector?

My main recommendation — and this has been a recurring theme — is maintaining a collaborative approach in order to gain a strategic advantage in today's complex risk landscape. All levels of government and industry have to come together to develop plans and solutions that address cybersecurity and reduce other systemic risks to our digital infrastructure.

The need for a collaborative approach can't be overstated. Agencies that work with industry partners as closely as CISA does truly understand the importance of this approach. ■