Continuing to Strengthen International Connections on the Cybersecurity Framework

In these uncertain times, our most important focus is on health and safety. Like so many of you, most of us at NIST are working remotely. But we are still working hard to support our cybersecurity mission. While NIST had to cancel the Advancing Cybersecurity Risk Management Conference scheduled for May 2020, we look forward to continuing our cybersecurity efforts through virtual meetings and discussions with you. We continue our international work and welcome your feedback on how we can strengthen our engagement in different and creative ways. After all, our international connections are more important than ever.

This was one of the very clear messages NIST received when we first convened stakeholders in 2013 to discuss a potential Cybersecurity Framework. We were asked to ensure that it be aligned with other cybersecurity approaches used in all the places U.S. organizations operate. We are fortunate to be able to continue engaging with stakeholders to improve international awareness of and engagement with the Framework, which will also help us improve the Framework.

Since our last update for Cybersecurity Awareness Month, I had the opportunity to work with some of our international peers during a six-week work detail in Vienna, Austria, as part of the Department of State's Embassy Science Fellows program. While at the U.S. Tri-Mission Vienna Embassy, I focused on cybersecurity policy and collaboration as part of the U.S.-Austria Strategic Dialogue, which was launched in February 2019. This detail aligned well with my role in engaging internationally to support the Cybersecurity Framework and NIST's broader cybersecurity risk management approaches.

During my time in Vienna, I met with key players in Austria's cybersecurity landscape, including representatives from various ministries, industry groups, research institutions and universities. I learned through these conversations about cybersecurity and critical infrastructure protection efforts in Austria and shared information about NIST resources, including the Cybersecurity Framework.

I'm grateful to the Political Economic section of the U.S. Tri-Mission Embassy in Vienna and all those I spent time with for the amazing opportunity to work on this project and to lay the groundwork for continued collaboration. I also owe a debt of gratitude to the Office of Science and Technology Austria at the Austrian embassy in Washington, D.C., for helping me to prepare for my detail and for the continued engagement upon my return. I look forward to working with all of these colleagues on future opportunities for cybersecurity collaboration, work that has no doubt been enhanced by my time spent in Austria. I'm also excited to use this experience to advance NIST's international work on the Cybersecurity Framework and other programs. Much of what I discussed with colleagues in Vienna will be valuable in better understanding how others around the globe view the Framework and other NIST cybersecurity efforts. These and other international engagements help to support our efforts to improve alignment.

I am pleased to report that NIST has seen an increase in the number of translations of the Framework, including a soon-to-be available Bulgarian translation. All translations and adaptations are available on our recently reorganized Framework International Resources site. We continue to add other resources related to the Framework to the site, including a white paper from the Coalition to Reduce Cyber Risk (CR2) on elevating global cybersecurity risk management through interoperable frameworks.

Our NIST team wishes everyone health and safety, and we look forward to continuing to engage even more meaningfully (if virtually) with our partners in the coming weeks and months to work toward greater alignment of cybersecurity standards, guidelines and best practices. Please reach out to me at amy.mahn@nist.gov with any questions or suggestions.

ABOUT THE AUTHOR

Amy Mahn

Amy Mahn is an international policy specialist in the NIST Applied Cybersecurity Division. Amy's primary focus in this role is support of the international aspects and alignment of the Framework for Improving Critical Infrastructure Cybersecurity. Amy previously worked eleven years at the Department of Homeland Security in various roles, including international policy coordination in cybersecurity and critical infrastructure protection within the National Protection and Programs Directorate and the Office of Cyber, Infrastructure and Resilience Policy.