Bill, as always thank you so much for the opportunity to submit the request for a new work role. Attached is the updated version with input from our community. Everyone on our end is really excited about this, so thanks for making this RFC happen :)

Thanks!

Lance Spitzner
Director, Research and Community

The Security Awareness Summit 5/6 August in Austin, TX. https://www.sans.org/SecAwareSummit

NIST NICE Work Role Description – Security Awareness & Engagement Manager

The NIST NICE Framework (SP800-181) is a formalized approach to defining the Cybersecurity Workforce. The purpose of the framework is to enable organizations to effectively identify, hire, track, and develop a qualified cybersecurity workforce. In addition, the framework enables those who wish to enter the Cybersecurity workforce better understand their options or helps those already in the workforce define and develop their career path. The framework does this by creating a common lexicon, ultimately identifying different Work Roles, what you and I would call job descriptions. NIST NICE defines each Work Role with a title and description, Tasks expected for that Work Role , and the Knowledge, Skills and Abilities (KSAs) required for the Work Role. This ensures that everyone is speaking the same language. For example, if you need to hire someone for your Incident Response team, you can provide the exact requirements for an Incident Responder to your Human Resources team based on the framework. Similarly, people looking to be hired in such a position know exactly what is expected of them.

Such a framework is powerful until you run into a role that is not identified by the framework. After reviewing the NICE Framework we could not find what we felt was a good description for what we call a Security Awareness and Engagement Manager. This is someone who's target audience is the entire workforce and focuses primarily behavior and culture change. The closest Work Roles we could find were

- Cyber Instructional Curriculum Developer (OV-TEA-001)
- Cyber Instructor (OV-TEA-002)
- Cyber Workforce Developer and Manager (OV-SPP-001)

While all three of these had elements that could make up Security Awareness, none of them are a good fit. The first two Work Roles are focused on creating and implementing technical, skills-based training for specialized roles. In other words, most often training security professionals to become more technical and advanced security professionals. Security Awareness can focus on developing technical security skills such as for IT Admins or Developers, however it's more often about creating secure behaviors in your entire workforce. It's about creating a security mindset / culture throughout the organization. In many ways Security Awareness is about organizational change, requiring very different skill sets. As such, we came up with what we feel is a better description for someone involved in Security Awareness, Engagement and Culture related activities.

Work Role Name	Security Awareness & Engagement Manager
Work Role ID	OV-TEA-003
Specialty Area	Training, Education and Awareness (TEA)
Category	Oversee and Govern (OV)
Work Role Description	Builds, maintains and measures the organizations security awareness and communications program with the goal of securing the workforce's behaviors and ultimately creating a secure culture.
Tasks	T0001, T0024, T0025, T0030, T0073, T0094, T0101, TO157, T0206,T0224, T0248, T0316, T0320, T0321, T0322, T0323, T0341, T0345, T0352, T0357, T0365, T0367, T0380, T0382, T0384, T0425, T0437, T0442, T0443, T0450, T0451, T0467, T0519, T0520, T0534, T0535, T0926
Knowledge	K0002, K0004, K0115, K0124, K0204, K0208, K0213, K0215, K0216, K0217, K0218, K0220, K0226, K0239, K0243, K0245, K0250, K0252, K0628,
Skills	S0052, S0070, S0100, S0101, S0296, S0301, S0356
Abilities	A0004, A0006, A0011, A0012, A0013, A0014, A0016, A0017, A0018, A0020, A0022, A0057, A0070, A0083, A0089, A0105, A0106, A0114, A0119, A0171

You will notice that the biggest difference is we have removed most of the Tasks and KSA's that are highly technical focused, with an emphasis on softer skills such as communications, partnering, behavior modeling, engagement and project management. For example, a key model many Security Awareness managers leverage is the BJ Fogg Behavior Model or organizational change models such Prosci ADKAR. We have often found the best Security Awareness managers come from soft-skills backgrounds, such as Marketing, Communications, Public Relations, Sales or Journalism. By partnering and working with members of the technical Security Team, Security Awareness professionals can then leverage that team's expertise and 'translate' that into learning objectives, content and training modalities that the workforce can readily consume and act on.

We have repeatedly identified in the annual Security Awareness Report that most organizations treat human security at best as a part time role, often a role simply dumped on someone within the technical security team. And yet reports like the Verizon DBIR continue to identify the human as one of the primary attack vectors and organizations greatest risk. We hope by adopting this Work Role, NIST NICE Framework will encourage more organizations to invest in a dedicated role responsible for organization wide awareness and behavior change, with the proper skills and background. In addition, this new Work Role is ultimately defined by the community for the community.