Please consider this a formal proposal from the SANS Institute on some additional work roles we would like to propose into the 2020 NICE Framework. These work roles were put together by our industry practitioners and experts on real world jobs that we believe are missing on today's framework:

Industrial Control Systems/SCADA – New Category

- Process Control Engineer / Instrument & Control Engineer
- ICS/SCADA Security Engineer
- ICS/OT Systems Engineer
- OT SOC Operator

Vulnerability Assessment and Management (VAM) – Current Category

- Pen Tester
- Adversary Emulation Specialist / Red Teamer

We have built these proposals in the same format as the current NICE Framework to make it easy for review.

Please also let me know how I can provide any additional information and thanks ahead on your consideration!

Brian Correia
Director of Workforce Development

http://www.sans.org

At **SANS Security East 2020,** gain practical cybersecurity skills you can implement immediately! Join us **New Orleans**, **February 1-8**, and choose from over 30 courses, plus three types of NetWars, multiple bonus talks, and several career-enhancing networking opportunities.

"SANS training is the real deal. Real-world attacks are broken down with tools you can use come Monday." - Tim Wesley, Hillenbrand, Inc.

NICE Framework Specialty Areas and Work Role Table of Contents

11/15/2019

Nice Framework Version 1/18/18

NICE Specialty Area	NICE Specialty Area Definition	Work Role	Work Role Definition	Work Role ID	OPM Code (Fed Use)
Industrial Control Systems (NICE 2020)					
Operations Technology Engineering	Interacts with, operates, or supports Industrial Control or Operations Technology Systems. Training program may introduce ICS, the risks or types of ICS attacks, basic system and network defenses and controls, as well as typical ICS governance and policy best practices. Program goal should change human behavior in an OT/ICS environment and reduce risk.	Process Control Engineer / Instrument & Control Engineer	Process control engineers design, test, troubleshoot, and oversee implementation of new processes. In plants with established control systems, the engineers may design and install retrofits to existing systems and troubleshoot hardware, software, and instrument problems in a manner that also preserves the cyber integrity of the environment.		
		ICS/SCADA Security Engineer	Monitor and protect industrial control system environments with the goal of keeping the operational environment safe, secure, and resilient against current and emerging cyber threats.		
		ICS/OT Systems Engineer	Designs, builds, and supports computer systems to support the operations environment.		
OT Security Operations Center	A centralized unit from where staff supervises operations technology environment with the goal of detecting, analyzing, and responding to cybersecurity incidents.	OT SOC Operator	Identifies, collects, examines, and preserves evidence form OT / ICS environments using controlled and documented analytical and investigative techniques that minimize the impact to the operations environment.		

NICE Framework Specialty Areas and Work Role Table of Contents

11/15/2019	Nice Framework Version 1/18/18				
NICE Specialty Area	**NICE Specialty Area Definition**	**Work Role**	**Work Role Definition**	**Work Role ID**	**OPM Code (Fed Use)**
Vulnerability Assessment and Management (VAM)	Conducts assessments of threats and vulnerabilities; determines deviations from acceptable configurations, enterprise or local policy; assesses the level of risk; and develops and/or recommends appropriate mitigation countermeasures in operational and nonoperational situations.	*Vulnerability Assessment Analyst*	*Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.*	*PR-VAM-001*	*541*
		Pen Tester	This expert finds security vulnerabilities in target systems, networks, and applications in order to help enterprises improve their security. By identifying which flaws can be exploited to cause business risk, the pen tester provides crucial insights into the most pressing issues and suggests how to prioritize security resources.		
		Adversary Emulation Specialist / Red Teamer	A security expert who emulates how an adversary operates using TTPs (Tactics, Techniques & Procedures). The goal is to improve how resilient the organization is versus these adversary techniques in order to prevent, detect, and respond accordingly.		

*Blue Italics is Current NICE Role