

Homeland Security Challenge

Strengthen the overall security posture of the nation by better preparing the current and future cybersecurity workforce.

Motivation & Goal

The motivation for this project is based on the large fairly complex corpus of frameworks used throughout industries. There seems to be a lack of frameworks dedicated to cybersecurity workforce (CSW) development. The goal of this project is to identify and analyze the differences and similarities of CSW frameworks while providing clarity to the literature.

Approach / Methodology

Surveyed a large portion of the available literature related to frameworks. Initial collection was intentionally broad to ensure those frameworks that may be applied toward CSW development were analyzed. Initially, 16 CSW related frameworks are identified and reduced to six based on the major functions and their popularity.

These six provided met the established criteria for this project, being focused on CSW development. The frameworks identified as relating to both cybersecurity and workforce development are 181 & 181r, DoDD 8140, CCM, NCAE, and COBIT.

Outcomes / Results

Frameworks were analyzed based on four key elements; publishing organization, goal/objective, audience, and mapping components and summarized in Table 1. The volume of text was large, but the analysis was conducted manually by hand. The effort involved in automated text analysis was reserved.

Through the initial identification resulted in a wide assortment of frameworks we are confident the resulting analysis incorporates many relevant frameworks.

Table 1: CSW Framework Analysis Summary Results

	NICE Cybersecurity Workforce Framework (NCWF) - NIST SP 800-181 in 2017	NICE CWF- NIST SP 800-181r1 in 2020	DoDD 8570/8140 Cyber Workforce Framework	National Centers of Academic Excellence in Cyber Defense/Cyber Operations (CAE-CD/CO)	Cybersecurity Competency Model	ISACA COBIT
Initiative organization	NIST (National Institute of Standard and Technology)	NIST	DoD (Department of Defense)	NSA	Department of Labor	Information Systems Audit and Control Association
Goal/Objective	Describes and categorizes cybersecurity work and identifies sample job titles, tasks, and KSAs (Knowledge, skills, and Abilities)	Describes cybersecurity work and learners implemented through a modular building block approach comprised of Tasks, Knowledge, and Skills	Provides the foundation for identifying education, training, and certification requirements to support cybersecurity personnel qualification	Promotes the focus of cybersecurity in higher education curriculum and research Aims to produce professionals with Cyber Operations (CO) and Cyber Defense (CD) expertise in various disciplines	Provide a comprehensive overview of cybersecurity workforce competencies, including roles, training, and career paths for job seekers.	Provide guidance for businesses to develop and organize, and implement strategies regarding information management and technology
Main Audience	<ul style="list-style-type: none"> Employers Current/Future Cybersecurity workers Training/Certification Programs Educators Technology Providers 	<ul style="list-style-type: none"> Employers Organizations, public and private Educators/Trainers Students and those looking to enter the field 	<ul style="list-style-type: none"> Military, civilian, and contractor cybersecurity personnel Training vendors, certification bodies, colleges, and continuing education providers 	<ul style="list-style-type: none"> 2-year, 4-year, and graduate-level institutions in the U.S. seeking CAE designations 	Current and future workforce (generally unemployed or under employed) participants, as well as employers, who need guidance on work role-KSA congruity	Businesses IT and Assurance, historically the financial sector, helps provide insight to senior management
Mapping Components	<ul style="list-style-type: none"> 7 Categories (Securely, Provision, Protect and Defend, Investigate, College and Operate, analyze, Operate and Maintain, Oversee and Govern) 33 Specialty Areas 52 Work Roles (KSA) 	(New TKS in Draft Previous NIST components valid until further publication) Nov 2021	<ul style="list-style-type: none"> DoD work roles, tasks, functions and baseline KSAs Under development awaiting DoD 8140.01 Manual 33 Specialty Areas, 54 Work Roles 	<ul style="list-style-type: none"> 3 Foundational KUs 5 Core Technical KUs 5 Core Non-Technical KUs 57 Optional KUs 	<ul style="list-style-type: none"> 5 base tiers - pyramid structure, tapering from general 'soft' skills and responsibilities to specialized competency areas at the top Utilizes NICE Framework (NCWF), KSAs - 52 work roles 	<ul style="list-style-type: none"> 3 Focus areas: Devops, IT Risk, Security 6 Governance Principles 3 Framework Principles 5 Domains (Government and Management Objectives)
Highlights	<ul style="list-style-type: none"> Backed by NIST Large target audience Biggest mapping component 	<ul style="list-style-type: none"> 181r provides a simplified and flexible approach to describe cybersecurity work Able to be utilized by a wide range of users 	<ul style="list-style-type: none"> Small target audience 8140.01 Manual not released yet Strict guidelines and requirements 	<ul style="list-style-type: none"> 100% Academia focused Technical/Non-technical KUs 2nd Biggest mapping component 	<ul style="list-style-type: none"> Similar structure as NICE Large target audience Catered toward newer workforce participants 	Main focus on management and enterprise governance

Discussions

There are similarities among the reported six frameworks. All the frameworks exhibit a goal of developing a cybersecurity workforce. They all utilize some variation of knowledge, skills, and tasks. They also share a common foundation in or contain and large component of the NICE Framework.

We have developed a simple yet effective template for which future iterations of and new published frameworks can be quickly evaluated by audiences to gauge the relevance of a particular framework or update.

Comparing the cybersecurity workforce frameworks provides the ability to better understand the current frameworks and their application. This subjacent project constructed the foundation for continued research whereby knowledge, skills, and tasks were extracted from job postings and compared to the NICE Framework.

Selected References

1. National Institute of Standards and technology, (2020, November), *NIST Special Publication 800-181 Revision 1*, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>
2. National Institute of Standards and technology, (2021, April 13), *Task Knowledge Skill (TKS) Statements Authoring Guide for Workforce Frameworks*, https://www.nist.gov/system/files/documents/2021/04/13/TKS_Authoring_Guide13apr2021-508Compliant.pdf
3. National Institute of Standards and technology, (2021, March), *NICE Framework Competencies: Assessing Learners for Cybersecurity Work*, <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8355-draft.pdf>

Acknowledgements

This research was performed under an appointment to the U.S. Department of Homeland Security (DHS) Science & Technology (S&T) Directorate Office of University Programs Summer Research Team Program for Minority Serving Institutions, administered by the Oak Ridge Institute for Science and Education (ORISE) through an interagency agreement between the U.S. Department of Energy (DOE) and DHS. ORISE is managed by ORAU under DOE contract number DE-SC0014664. All opinions expressed in this paper are the author's and do not necessarily reflect the policies and views of DHS, DOE or ORAU/ORISE.