

# NICE Cybersecurity Workforce Framework

## NIST Special Publication 800-181

### WHY?

The NICE Cybersecurity Workforce Framework (NICE Framework) improves communication about how to identify, recruit, develop, and retain cybersecurity talent. It is a resource from which organizations or sectors can develop additional publications or tools that meet their needs to define or provide guidance on different aspects of workforce development, planning, training, and education.

### PURPOSE

This publication serves as a fundamental reference to support a workforce capable of meeting an organization's cybersecurity needs. It provides organizations with a common, consistent lexicon that categorizes and describes cybersecurity work by Category, Specialty Area, and Work Role. It provides a superset of cybersecurity Knowledge, Skills, and Abilities (KSAs) and Tasks for each work role. The NICE Framework supports consistent organizational and sector communication for cybersecurity education, training, and workforce development.

### DEVELOPMENT

The concept for the NICE Framework began before the establishment of NICE and grew out of the recognition that the cybersecurity workforce in both the public and private sectors could not be defined and assessed. To address this challenge, more than 20 departments and agencies, the private sector, and academia came together to provide a common understanding of cybersecurity work. The common understanding developed has been expressed in two previous versions of the NICE Framework and has evolved with further engagement between the government, private sector, and academia.

### LEARN MORE

[nist.gov/nice/framework](https://nist.gov/nice/framework)

### AUDIENCE

**Employers** - to help define their cybersecurity workforce, identify critical gaps in cybersecurity staffing, and create position descriptions consistent with national language.

**Current and Future cybersecurity workers** - to help explore Tasks and Work Roles and assist with understanding the KSAs that are being valued by employers for in-demand cybersecurity jobs and positions. Staffing specialists and guidance counselors are also enabled to use the NICE Framework as a resource to support these employees or job seekers.

**Training and certification providers** - to help current and future members of the cybersecurity workforce gain and demonstrate the KSAs.

**Education providers** - to help develop curriculum, certificate or degree programs, and research that cover the KSAs and Tasks described.

**Technology providers** - to identify cybersecurity Work Roles and specific Tasks and KSAs associated with services and hardware or software products they supply.

### DEFINITIONS

**Categories:** A high-level grouping of common cybersecurity functions

**Specialty Areas:** Represent an area of concentrated work, or function, within cybersecurity and related work

**Work Roles:** The most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of a list of knowledge, skills, and abilities (KSAs) and a list of tasks performed in that role

**Tasks:** Specific work activities that could be assigned to an individual working in one of the NICE Framework's Work Roles

**KSAs:** Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training



SECURELY  
PROVISION



OPERATE &  
MAINTAIN



OVERSEE &  
GOVERN



PROTECT &  
DEFEND



ANALYZE



COLLECT &  
OPERATE



INVESTIGATE