

Draft (2nd) NISTIR 8355

NICE Framework Competencies:

Assessing Learners for Cybersecurity Work

Karen A. Wetzel

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8355-draft2>

NICE Framework Competencies:

Assessing Learners for Cybersecurity Work

Karen A. Wetzel (Manager of the NICE Framework)
National Initiative for Cybersecurity Education (NICE)
Applied Cybersecurity Division
Information Technology Laboratory

This publication is available free of charge from:
<https://doi.org/10.6028/NIST.IR.8355-draft2>

December 2021



U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
*James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce
for Standards and Technology & Director, National Institute of Standards and Technology*

48 National Institute of Standards and Technology Interagency or Internal Report 8355
49 18 pages (December 2021)

50 This publication is available free of charge from:
51 <https://doi.org/10.6028/NIST.IR.8355-draft2>

52 Certain commercial entities, equipment, or materials may be identified in this document in order to describe an
53 experimental procedure or concept adequately. Such identification is not intended to imply recommendation or
54 endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best
55 available for the purpose.

56 There may be references in this publication to other publications currently under development by NIST in accordance
57 with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies,
58 may be used by federal agencies even before the completion of such companion publications. Thus, until each
59 publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For
60 planning and transition purposes, federal agencies may wish to closely follow the development of these new
61 publications by NIST.

62 Organizations are encouraged to review all draft publications during public comment periods and provide feedback to
63 NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at
64 <https://csrc.nist.gov/publications>.

65

66 **Public comment period: *December 15, 2021 through January 31, 2022***

67 **Email: NICEFramework@nist.gov**

68 National Institute of Standards and Technology

69 Attn: Applied Cybersecurity Division, Information Technology Laboratory

70 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

71 All comments are subject to release under the Freedom of Information Act (FOIA).

72

73

Reports on Computer Systems Technology

74 The Information Technology Laboratory (ITL) at the National Institute of Standards and
75 Technology (NIST) promotes the U.S. economy and public welfare by providing technical
76 leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test
77 methods, reference data, proof of concept implementations, and technical analyses to advance the
78 development and productive use of information technology. ITL's responsibilities include the
79 development of management, administrative, technical, and physical standards and guidelines for
80 the cost-effective security and privacy of other than national security-related information in federal
81 information systems.

82

Abstract

83 This publication from the National Initiative for Cybersecurity Education (NICE) describes
84 Competencies as included in the *Workforce Framework for Cybersecurity (NICE Framework)*,
85 NIST Special Publication 800-181, Revision 1, a fundamental reference for describing and
86 sharing information about cybersecurity work. The NICE Framework defines Task, Knowledge,
87 and Skill (TKS) statement building blocks that provide a foundation for learners, including
88 students, job seekers, and employees. Competencies are provided as a means of applying those
89 core building blocks by grouping related TKS statements to form a higher-level statement of
90 competency. This document shares more detail about what Competencies are, including their
91 evolution and development. Additionally, the publication provides example uses from various
92 stakeholder perspectives. Finally, the publication identifies where the NICE Framework list of
93 Competency Areas is published separate from this publication and provides the rationale for why
94 they will be maintained as a more flexible and contemporary reference resource.

95

Keywords

96 Competency; Competency Area; cyber; cybersecurity; cyberspace; education; knowledge; risk
97 management; role; security; skill; task; team; training; workforce; work role.

98

99

Acknowledgments

100 The National Institute of Standards and Technology (NIST) would like to particularly
101 acknowledge the work of William Newhouse (NIST), Kevin Sanchez-Cherry (Department of
102 Transportation), Leo Van Duyn (JP Morgan Chase & Co.), and Clarence Williams (Department
103 of Veterans Affairs), whose work provided the basis from which this publication came. NIST
104 also wishes to thank these team members from the NICE Framework Core Authoring Team that
105 includes representatives from numerous departments and agencies in the United States federal
106 government whose dedicated efforts contributed significantly to that publication:

107

108 Lisa Dorr, Department of Homeland Security

109 Ryan Farr, Department of Defense

110 Pam Frugoli, Department of Labor

111 Matt Isnor, Department of Defense

112 Patrick Johnson, Department of Defense

113 Rodney Petersen, National Institute of Standards and Technology

114 Danielle Santos, National Institute of Standards and Technology

115 Stephanie Shively, Department of Defense

116 Kenneth Vrooman, Cybersecurity and Infrastructure Security Agency

117 Finally, the team appreciates and acknowledges the contributions of those who established
118 previous editions of cybersecurity workforce frameworks as described at the History page of the
119 [NICE Framework Resource Center](#).

120

121

Audience

122 The NICE Framework serves as a bridge between employers and education and training
123 providers as well as a tool to help learners determine needs and demonstrate capabilities.
124 Providing a standardized approach to Competencies provides direct information about what a
125 workforce needs to know, enables the development of more effective learning, and establishes
126 regular processes to consistently describe and validate a learner's capabilities. Therefore,
127 employers, workforce development and human resources professionals, education and training
128 providers, learners, and others are stakeholders and the audience for this work.

129

Document Conventions

130 The terms “shall” and “shall not” indicate requirements to be followed strictly in order to
131 conform to the publication and from which no deviation is permitted. The terms “should” and
132 “should not” indicate that among several possibilities one is recommended as particularly
133 suitable, without mentioning or excluding others, or that a certain course of action is preferred
134 but not necessarily required, or that (in the negative form) a certain possibility or course of action
135 is discouraged but not prohibited. The terms “may” and “need not” indicate a course of action
136 permissible within the limits of the publication. The terms “can” and “cannot” indicate a
137 possibility and capability, whether material, physical or causal.

138 Those performing cybersecurity work—including students, job seekers, and employees—are
139 referenced as Learners. This moniker highlights that each member of the workforce is also a
140 lifelong learner.

141

Note to Reviewers

142 This draft publication assumes some existing knowledge of the NICE Framework and is
143 expected to be read in that context. This is the second draft of this document. The first draft was
144 released in March 2021 along with an initial list of proposed Competency Areas. Feedback
145 received on that first draft, conversations with NICE community members, and insights from
146 workshops that brought together subject matter experts have matured our understanding of NICE
147 Framework Competencies. The adjustments to this document are the result. In addition, we will
148 be working with community stakeholders to further refine the proposed list of Competency
149 Areas for release in 2022. Any subsequent draft(s) may be further adjusted, including the
150 Competency Areas, their descriptions, and associated Task, Knowledge, and Skill (TKS)
151 statements.

152

Call for Patent Claims

153 This public review includes a call for information on essential patent claims (claims whose use
154 would be required for compliance with the guidance or requirements in this Information
155 Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be
156 directly stated in this ITL Publication or by reference to another publication. This call also
157 includes disclosure, where known, of the existence of pending U.S. or foreign patent applications
158 relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

159

160 ITL may require from the patent holder, or a party authorized to make assurances on its behalf,
161 in written or electronic form, either:

162

163 a) assurance in the form of a general disclaimer to the effect that such party does not hold
164 and does not currently intend holding any essential patent claim(s); or

165

166 b) assurance that a license to such essential patent claim(s) will be made available to
167 applicants desiring to utilize the license for the purpose of complying with the guidance
168 or requirements in this ITL draft publication either:

169

170 i. under reasonable terms and conditions that are demonstrably free of any unfair
171 discrimination; or

172

173 ii. without compensation and under reasonable terms and conditions that are
174 demonstrably free of any unfair discrimination.

174

175 Such assurance shall indicate that the patent holder (or third party authorized to make assurances
176 on its behalf) will include in any documents transferring ownership of patents subject to the
177 assurance, provisions sufficient to ensure that the commitments in the assurance are binding on
178 the transferee, and that the transferee will similarly include appropriate provisions in the event of
179 future transfers with the goal of binding each successor-in-interest.

180

181 The assurance shall also indicate that it is intended to be binding on successors-in-interest
182 regardless of whether such provisions are included in the relevant transfer documents.

183

184 Such statements should be addressed to: niceframework@nist.gov

185

186

187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204

Table of Contents

1 Introduction 1

 1.1 Purpose 1

 1.2 Scope..... 1

2 Competencies and the NICE Framework 2

 2.1 Evolution of NICE Framework Competencies..... 2

 2.2 Defining Competencies..... 3

 2.2.1 Developing Competency Statements 4

 2.2.2 Example uses 5

References 8

List of Appendices

Appendix A— Acronyms 9

Appendix B— Glossary 10

205 **1 Introduction**

206 The *Workforce Framework for Cybersecurity (NICE Framework)*, NIST Special Publication
207 800-181, Revision 1, was released in November 2020 [1]. This revision establishes at the core of
208 the NICE Framework a set of building blocks – Tasks, Knowledge, and Skills – as well as
209 identifies common ways that the Framework can be applied, most notably through Work Roles
210 and, new in this revision, Competencies (see Appendix 1: Evolution of NICE Framework
211 Competencies). The NICE Framework building blocks, Work Roles, and Competencies will be
212 maintained separately and made available as part of the [NICE Framework Resource Center](#) in
213 order to allow for regular review and updates [2].

214 Competencies are a means to apply the NICE Framework core building blocks by grouping
215 related Task, Knowledge, and Skill (TKS) statements to form a higher-level statement of
216 competency. They further provide a means of learner—which, for the purposes of the NICE
217 Framework includes students, job seekers, and employees—assessment by clearly defining what
218 a person needs to know and be able to do to perform well in a defined area of cybersecurity
219 work. They are defined via an employer-driven approach that provides insight to an
220 organization’s unique context. Because of this, they also allow education and training providers
221 to be responsive to employer or sector needs by creating learning experiences that help learners
222 develop and demonstrate the Competencies. For the purposes of the NICE Framework, a
223 Competency is a measurable cluster of related Task, Knowledge, or Skill statements in a
224 particular domain that correlates with performance on the job and can be improved through
225 education, training (including on-the-job or via apprenticeships), or other learning experiences.

226 **1.1 Purpose**

227 This publication introduces readers to NICE Framework Competencies and why they were
228 introduced in the revised NICE Framework publication; describes how the Competencies are
229 defined and written; and shares with readers ways NICE Framework Competencies can be used.

230 **1.2 Scope**

231 The Competencies defined in this publication are for use with the *Workforce Framework for*
232 *Cybersecurity (NICE Framework)*, which provides a lexicon for describing cybersecurity work
233 and the individuals who do that work. The NICE Framework considers the “cybersecurity
234 workforce” to include not only those whose primary focus is on cybersecurity but also those who
235 need specific cybersecurity-related knowledge and skills to properly manage cybersecurity-
236 related risks to the enterprise.

237 **2 Competencies and the NICE Framework**

238 The introduction of Competencies into the NICE Framework is a response to a growing need for
239 a skilled cybersecurity workforce. Indeed, private sector employers have already begun shifting
240 to meet needs, including modernizing recruitment practices to better identify and secure talent
241 through skills- and competency-based hiring. Hiring based only on degrees increases the
242 likelihood to exclude qualified candidates, particularly for jobs related to emerging technologies,
243 and a shift to competency-based hiring and promotion ensures that the individuals most capable
244 of performing the roles and responsibilities required of a specific position are those selected for
245 that position. The introduction of Competencies into the NICE Framework thereby provides a
246 means of helping the multiple NICE Framework audiences shift in this direction.

247 Competencies offer flexibility by allowing organizations to group together various Tasks,
248 Knowledge, and Skills (TKS) statements into overarching areas that define a broad need. While
249 an individual Task and its associated Knowledge and Skill statements may not change, a
250 Competency Area may require the introduction of new Tasks or even individual Knowledge and
251 Skills—or remove existing ones—in response to evolving needs in a changing cybersecurity
252 ecosystem. NICE Framework Competencies are complementary to Work Roles and provide a
253 means to assess learner capabilities in the defined areas.

254 **2.1 Evolution of NICE Framework Competencies**

255 NICE Framework Competencies were first introduced in the 2020 revision of that publication
256 but derive from earlier work. The first version of the [National Cybersecurity Workforce
257 Framework 1.0 - Interactive PDF](#) (April 2013), which preceded and formed the basis for NIST
258 SP 800-181, included a mapping of Knowledge, Skill, and Ability (KSA) statements to
259 competencies.¹ These competencies pulled from a 2011 U.S. Office of Personnel Management
260 (OPM) memorandum that introduced a “[Competency Model for Cybersecurity](#),” which itself
261 followed a coordinated effort with the Federal Chief Information Officers (CIO) Council and
262 NICE in November 2009.² The OPM model presented 117 competencies related to four
263 occupation series and the pay grades of personnel in those occupations. A subject matter expert
264 panel review of the OPM model conducted at that time identified 50 competencies to align with
265 the NICE Framework KSAs found in five of the seven categories of work.³

266 Prior to publishing NIST SP 800-181 in 2017, consideration was given as to whether
267 competencies should be maintained in that version. It was determined at that time to not include
268 them in part due to what was felt a need for additional work to provide adequate definitions of
269 the competencies as well as to address inconsistencies with the KSA alignment. When revising

¹ Note that Ability statements were removed in the 2020 revision of the NICE Framework.

² Berry, J. (2011, February 16). U.S. Office of Personnel Management Memorandum. Competency model for cybersecurity. Retrieved February 11, 2021, from <https://www.chcoc.gov/content/competency-model-cybersecurity> [4]

³ Two categories—“Collect and Operate” and “Analyze”—related to classified content and thus were not included in that alignment review.

270 the NICE Framework in 2019-2020, inclusion of competencies was revisited and then included
271 in the 2020 publication.

272 **2.2 Defining Competencies**

273 Competencies offer a higher-level perspective on
274 cybersecurity work, allowing organizations to bring
275 together various TKS statements for a defined area of
276 cybersecurity work. As hiring becomes more inclusive of
277 competencies in determining capabilities, applicant pools
278 are broadened to identify candidates more successfully,
279 particularly in areas such as emerging and rapidly
280 evolving technologies. They offer an assessment-based
281 approach to hiring and promotion, in determining career
282 paths, for identifying current gaps and future needs, and in
283 aligning education and training goals. A Competency Area
284 consists of a name, description of the area, and group of
285 associated TKS statements. Importantly, they are:

Competency Area: A measurable cluster of related Task, Knowledge, or Skill (TKS) statements in a particular domain that correlates with performance on the job and can be improved through education, training (including on-the-job and via apprenticeships), or other learning experiences.

Competency Areas consist of a name, description of the area, and group of associated TKS statements.

- 286 • Defined via an employer-driven approach
- 287 • Learner-focused
- 288 • Observable and measurable

289 Accordingly, instead of specifying the work to be done (Tasks) or what is needed to do the work
290 (Knowledge and Skills), it’s about assessing a learner’s overall competency for that area of work
291 (the combination of TKS statements that it encompasses). Competencies offer an opportunity to
292 increase alignment and coordination between employers, learners, and education and training
293 providers (see Figure 1: NICE Competencies Stakeholders).

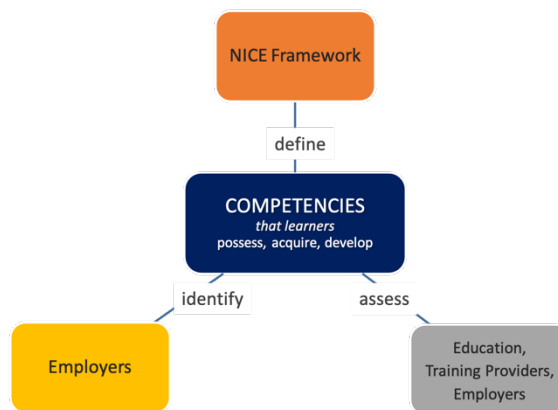


Figure 1: NICE Competencies Stakeholders

294

295 NICE Framework Competencies and Work Roles (which identify a group of tasks for which
296 someone is responsible) are complementary and may be used together or separately. However,
297 there are differences. While Competencies are learner-focused, Work Roles are work focused.
298 Competencies help address employer needs, while Work Roles are used when defining positions
299 and responsibilities. Finally, assessment is typically based on the Competency Area as a whole
300 (i.e., Task, Knowledge, and Skills), whereas assessment for Work Roles typically occurs at the
301 Task level.

Competencies

- Learner focused
- Help address employer needs
- Assessment is typically based on a Competency Area as a whole

Work Roles

- Work focused
- Help define positions and responsibilities
- Assessment typically occurs at the Task level

302 Finally, Competencies are flexible, allowing the inclusion or removal of individual TKS
303 statements in response to shifting needs in a changing cybersecurity ecosystem. As such, a listing
304 of defined NICE Framework Competency Areas will be maintained separate from this
305 publication and made available from the [NICE Framework Resource Center](#) as a more flexible
306 and contemporary reference resource.

307 2.2.1 Developing Competency Statements

308 The following guidelines are used for the development of individual Competency Areas as part
309 of the NICE Framework.

- 310 1. **Competency Area Title:** The name of the competency; the title should clearly signal to
311 all stakeholders the area that will be described.
- 312 2. **Competency Area Description:** The description should:
 - 313 a. **Begin with “This Competency Area describes a learner’s capabilities related
314 to....”** Using the same standard language to introduce each description serves as a
315 signpost for readers that it is a Competency Area description while focusing the
316 competency onto the learner at the onset.
 - 317 b. **Define the Competency Area simply and clearly.** Anyone reading the
318 description should be able to quickly and easily understand the scope and
319 meaning of the competency.
 - 320 c. **Reflect content from TKS statements.** The description may echo language from
321 Task, Skill, or Knowledge statements that are associated with the Competency
322 Area, though it should not wholly duplicate that language.
 - 323 d. **Balance specificity with broad application.** A goal of a NICE Framework
324 Competency Area is to provide flexibility of application; the description should

325 be detailed enough to clearly define its scope and meaning, but not so narrow as
326 to restrict use by multiple stakeholders or time-date the competency (e.g., by
327 referencing a particular computer program or coding language).

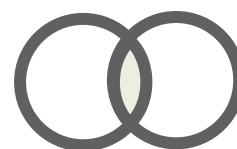
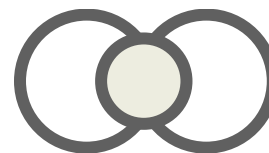
328 e. **Omit unnecessary qualifiers.** Qualifiers (e.g., “thorough knowledge,”
329 “considerable skill,” or “basic understanding”) and other proficiency level
330 indicators should not be included in the Competency description.

331 3. **Associated TKS Statements:** Each Competency Area will be associated with a defined
332 group of NICE Framework Task, Knowledge, and Skill statements that provide a more
333 detailed view of the Competency Area. Note that individual statements may be associated
334 with more than one Competency Area.

335 2.2.2 Example uses

336 The NICE Framework enables rapid adaptation to change while accounting for organizations’
337 unique operating contexts. At the same time, by establishing common language and approach, a
338 consistent exchange of cybersecurity workforce information is possible across an organization,
339 among multiple organizations, and sector wide. The Competencies extend the NICE
340 Framework’s attributes of agility, flexibility, interoperability, and modularity, which is reflected
341 in the multiple ways that they could be applied by its various stakeholders. There’s no one-size-
342 fits-all; they can be used in a variety of ways, including:

- **Overlaid on Work Role(s):** Additional capabilities may be necessary to effectively fulfill a Work Role. A position responsible for more than one Work Role may need the Competency Area across those roles (e.g., cloud security).
- **Common Ground:** A Competency Area can define unique cybersecurity capabilities needed by cybersecurity practitioners and other organizational staff to mitigate risks. In these cases, it serves as a common ground for communication and coordination (e.g., control systems cybersecurity).
- **Learning:** For students, job seekers, or employees, they can serve as a starting place for learning or a way to develop higher-level expertise in an area (e.g., digital forensics).



343 2.2.2.1 Employer Perspective

344 From an employer perspective, applications include:

- **Describe a given job:** Specific Competency Areas can be used when developing a job description or when defining a new role in an organization.

347 • **Track workforce capabilities:** Competency Areas can be used to broadly describe and
348 track an organization’s cybersecurity workforce capabilities, or an employer might look
349 at a grouping of Task, Knowledge, and Skills and define a custom Competency Area for
350 their unique needs.

351 • **Specify team requirements:** At times, a team needs to be formed before the individual
352 tasks the team will complete are defined. In these cases, the Competencies necessary to
353 solve a challenge can be used to identify team members, who will then determine the
354 specific work to be done.

355 • **Assess individual learner capabilities:** Learners can be assessed against various
356 Competency Areas at various or multiple stages, including as part of an interview, a
357 work-based learning evaluation, a promotion process, or career development.

358 2.2.2.2 Education, Training, or Credential Provider Perspective

359 From an education, training, or credential provider perspective, applications include:

360 • **In program development:** Providers could use a set of Competencies to develop a
361 learning program—bundling together related competencies—or differentiate levels of
362 proficiency within an individual Competency Area.

363 • **In course development:** Instructors might look at the most important Knowledge and
364 Skill statements reflected in a Competency Area to emphasize those statements in the
365 learning process.

366 • **In student assessment:** Providers could gauge whether learners have achieved
367 competency in a Competency Area before awarding a credential.

368 2.2.2.3 Learner Perspective

369 Finally, from the learner’s perspective, Competencies can be used at various stages and in
370 various ways, including to:

371 • **Assess one’s capabilities:** For example, to determine one’s overall competency in a
372 defined Competency Area.

373 • **Identify areas that may need development:** This can be done through assessment or by
374 using the Competency Area to self-identify areas that require further learning.

375 • **Learn about a defined area of expertise:** Competencies can offer a bird’s eye view for
376 anyone interested cybersecurity to help them understand needed expertise that may be
377 outside of defined Work Roles, as well as to connect a learner with details via the
378 associated TKS statements.

379 • **Understand an organization’s workforce needs:** For learners who are looking for a
380 new job, in a current job but wanting to make a shift, or are planning their career path,

381 Competencies can give insight into an organization's specific cybersecurity workforce
382 needs.

383 **References**

- 384 [1] Petersen R, Santos D, Wetzel K, Smith M, Witte G (2020). (National Institute of
385 Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181,
386 Rev. 1. <https://doi.org/10.6028/NIST.SP.800-181r1>
- 387 [2] National Institute of Standards and Technology (2021) *NICE Framework Resource*
388 *Center*. Available at <https://www.nist.gov/itl/applied-cybersecurity/nice/resources>
- 389 [3] Berry, J (2011) Competency model for cybersecurity. (U.S. Office of Personnel
390 Management, Washington, DC), U.S. Office of Personnel Management Memorandum,
391 February 16, 2021. Available at [https://www.chcoc.gov/content/competency-model-](https://www.chcoc.gov/content/competency-model-cybersecurity)
392 [cybersecurity](https://www.chcoc.gov/content/competency-model-cybersecurity)

393

394 **Appendix A—Acronyms**

395 Selected acronyms and abbreviations used in this paper are defined below.

CIO	Chief Information Officer
KSA	Knowledge, Skill, and Ability (KSA) statements
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OPM	Office of Personnel Management
TKS	Task, Knowledge, and Skill statements

396

397 **Appendix B—Glossary**

398 *The following identifies terms used in the NICE Framework and presents definitions in that*
 399 *context. For a complete glossary of terminology used in NIST's cybersecurity and privacy*
 400 *standards and guidelines, please visit <https://csrc.nist.gov/glossary>.*

401	Competency	A measurable cluster of related Task, Knowledge, or Skill (TKS) statements in a
402		particular domain that correlates with performance on the job and can be improved
403		through education, training (including on-the-job and via apprenticeships), or other
404		learning experiences.
405	Knowledge	A retrievable set of concepts within memory.
406	Skill	The capacity to perform an observable action.
407	Task	An activity that is directed toward the achievement of organizational
408		objectives.
409	Work Role	A way of describing a grouping of work for which someone is responsible or
410		accountable.