

**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-draft>

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15

**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-draft>

March 2021



U.S. Department of Commerce  
Gina 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 (March 2021)

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

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: *March 17, 2021 through May 3, 2021***

67 National Institute of Standards and Technology  
68 Attn: Applied Cybersecurity Division, Information Technology Laboratory  
69 100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000  
70 Email: [NICEFramework@nist.gov](mailto:NICEFramework@nist.gov)

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 to apply those core  
89 building blocks by grouping related TKS statements for 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  
93 Competencies list 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; cyber; cybersecurity; cyberspace; education; knowledge; risk management; role;  
97 security; skill; task; team; training; workforce; work role.

98

99

## Acknowledgments

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

108  
109 Lisa Dorr, Department of Homeland Security  
110 Ryan Farr, Department of Defense  
111 Pam Frugoli, Department of Labor  
112 Matt Isnor, Department of Defense  
113 Patrick Johnson, Department of Defense  
114 Rodney Petersen, National Institute of Standards and Technology  
115 Danielle Santos, National Institute of Standards and Technology  
116 Stephanie Shively, Department of Defense  
117 Kenneth Vrooman, Cybersecurity and Infrastructure Security Agency

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

121

122

## Audience

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

130

## Document Conventions

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

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

## 142 **Note to Reviewers**

143 This draft publication assumes some existing knowledge of the NICE Framework and is  
144 expected to be read in that context. In addition, it is to be understood that this is an initial draft  
145 and that subsequent draft(s) will not only incorporate feedback received from this public  
146 comment period but the associated Competencies list will be further defined as Competencies are  
147 grouped according to Task, Knowledge, and Skill (TKS) statements.

148 In addition to comments on the direct contents in this publication, please consider the following:

- 149 1) We would like to develop detailed use cases that can be used as implementation models.  
150 This document provides some high-level example uses, and it would be helpful to know  
151 if these are the primary use cases and what other might exist.
- 152 2) It will be important to distinguish uses cases for when NICE Framework Work Roles and  
153 Competencies might need to be used separately as well as when they can be used in  
154 tandem.
- 155 3) The accompanying NICE Framework Competencies list groups the Competencies by  
156 type (technical, operational, professional, or leadership). We are seeking to understand  
157 whether providing types is valuable and, if so, if the currently identified types meet  
158 needs.
- 159 4) Currently, the Competencies list includes some identified by the type “professional”—  
160 often thought of as employability or soft skills. Moving forward, we are seeking to  
161 understand how these important capabilities should be a part of Competencies; for  
162 instance, whether they should be:
  - 163 a. Included as NICE Framework Competencies, with associated TKS statements.
  - 164 b. Included as Knowledge or Skill statements that would be added to NICE  
165 Framework Competencies (note that TKS statements in the NICE Framework do  
166 not currently reflect professional capabilities).
  - 167 c. Not included directly; instead, the NICE Framework should simply reference  
168 other resources that provide details about professional capabilities that apply  
169 across multiple workforces.
- 170 5) Additionally, there are various existing professional skills models in existence, many of  
171 which were consulted in the development of the NICE Framework Competencies.  
172 Moving forward, we will need to determine if the Competencies should reference a single  
173 extant model should be used (and which one) or if multiple models should be assessed to  
174 determine which professional capabilities to integrate.

- 175 6) The NICE Program office would like to learn more about if and how proficiency levels  
176 (e.g., basic, intermediate, and advanced) should be incorporated into NICE Framework  
177 Competencies. It will be helpful to identify specific use cases around the use of  
178 proficiency levels and Competencies to help us better understand needs in this space,  
179 including references to extant models that should be considered in this effort.
- 180 7) NICE is in the process of defining a change process for regular updates and input in the  
181 NICE Framework components (Competencies, Work Roles, and TKS statements) to  
182 allow for adjustments to address, for instance, changes in technology and use. In addition,  
183 this process will be used to identify gaps (such as operational technology) that currently  
184 exist. Understanding more about gaps and how they can be addressed will be helpful in  
185 advance of our planning.

186

### Call for Patent Claims

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

193

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

196

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

199

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

203

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

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

208

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

214

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

217

218 Such statements should be addressed to: [niceframework@nist.gov](mailto:niceframework@nist.gov)

219

220



221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238

**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 ..... 7**

**List of Appendices**

**Appendix A— Acronyms ..... 8**

**Appendix B— Glossary ..... 9**

## 239 **1 Introduction**

240 The *Workforce Framework for Cybersecurity (NICE Framework)*, NIST Special Publication  
241 800-181, Revision 1, was released in November 2020 [1]. This revision establishes at the core of  
242 the NICE Framework a set of building blocks – Tasks, Knowledge, and Skills – as well as  
243 identifies common ways that the Framework can be applied, most notably through Work Roles  
244 and, new in this revision, Competencies (see Appendix 1: Evolution of NICE Framework  
245 Competencies). The NICE Framework building blocks, Work Roles, and Competencies will be  
246 maintained separately and made available as part of the [NICE Framework Resource Center](#) in  
247 order to allow for regular review and updates [2].

248 Competencies are a way to describe the assessment of a learner by clearly defining what a person  
249 needs to know and be able to do to perform well in a job or role. They are defined via an  
250 employer-driven approach that provides insight to an organization’s unique context. Because of  
251 this, they also allow education and training providers to be responsive to employer or sector  
252 needs by creating learning experiences that help learners develop and demonstrate the  
253 Competencies. For the purposes of the NICE Framework, a Competency is a measurable cluster  
254 of related task, knowledge, or skill statements that correlates with performance on the job and  
255 can be improved through education, training (including on-the-job or via apprenticeships), or  
256 other learning experiences.

### 257 **1.1 Purpose**

258 This publication introduces readers to NICE Framework Competencies; shares more about what  
259 competencies are and why they were reintroduced in the revised NICE Framework publication;  
260 describes how the Competencies were defined and written; and gives readers more information  
261 on how the NICE Framework can be used from a Competencies perspective.

### 262 **1.2 Scope**

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

## 269 **2 Competencies and the NICE Framework**

270 The reintroduction of Competencies into the NICE Framework is a response to a growing need  
271 for a skilled cybersecurity workforce. Indeed, private employers have already begun shifting to  
272 meet needs, including by modernizing recruitment practices to better identify and secure talent  
273 through skills- and competency-based hiring. Degree-based hiring is especially likely to exclude  
274 qualified candidates for jobs related to emerging technologies, and a shift to competency-based  
275 hiring and promotion ensures that the individuals most capable of performing the roles and  
276 responsibilities required of a specific position are those selected for that position. The  
277 introduction of Competencies is a means of helping the multiple NICE Framework audiences to  
278 shift in this direction.

279 Competencies offer flexibility by allowing organizations to group together various Tasks,  
280 Knowledge, and Skills (TKS) statements into an overarching groups that defines a broad need.  
281 While an individual Task and its associated Knowledge and Skill statements may not change, a  
282 more broadly defined Competency may require the introduction of new Tasks or even individual  
283 Knowledge and Skills — or remove existing ones — in response to evolving needs in a changing  
284 cybersecurity ecosystem.

285 The NICE Framework Competencies are a way for organizations to align with the NICE  
286 Framework at a high level without necessarily delving into the details of TKS statements,  
287 although the associated statements are available and can be referred to if desired. Competencies  
288 enable organizations to succinctly communicate and effectively organize their cybersecurity  
289 work in order to provide a streamlined view of the workforce.

### 290 **2.1 Evolution of NICE Framework Competencies**

291 The Competencies set forth in the 2020 NICE Framework publication derive from earlier work.  
292 The first version of the [National Cybersecurity Workforce Framework 1.0 - Interactive PDF](#)  
293 (April 2013), which preceded and formed the basis for NIST SP 800-181, included a mapping of  
294 Knowledge, Skill, and Ability (KSA) statements to competencies.<sup>1</sup> These competencies pulled  
295 from a 2011 U.S. Office of Personnel Management (OPM) memorandum that introduced a  
296 “[Competency Model for Cybersecurity](#),” which itself followed a coordinated effort with the  
297 Federal Chief Information Officers (CIO) Council and NICE in November 2009.<sup>2</sup> The OPM  
298 model presented 117 competencies related to four occupation series and the pay grades of  
299 personnel in those occupations. Following subject matter expert panel review of the OPM model,  
300 50 competencies were found to be aligned with the NICE Framework KSAs found in five of the  
301 seven categories of work.<sup>3</sup>

---

<sup>1</sup> Note that Ability statements were removed in the 2020 revision of the NICE Framework.

<sup>2</sup> 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]

<sup>3</sup> Two categories—“Collect and Operate” and “Analyze”—related to classified content and thus were not included in that

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

306 **2.2 Defining Competencies**

307 Ultimately, the NICE Framework defines Competencies  
 308 as a mechanism for organizations (including employers as  
 309 well as education and training organizations) to assess  
 310 learners. Competencies consist of a name, description of  
 311 the Competency, and group of associated TKS statements.  
 312 Importantly, they are:

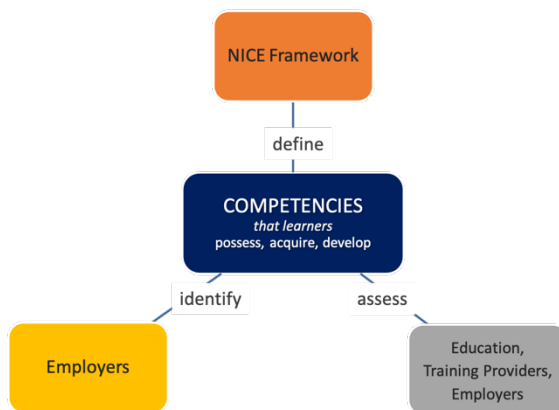
- 313 • Defined via an employer-driven approach
- 314 • Learner-focused
- 315 • Observable and measurable

**Competency: A mechanism for organizations to assess learners.**  
 Competencies consist of a name, description of the Competency, and group of associated TKS (Task, Knowledge, Skill) statements.

**Competencies are:**

- Defined via an employer-driven approach
- Learner-focused
- Observable and measurable

316 Accordingly, instead of specifying the work to be done  
 317 (Tasks) or what is needed to do the work (Knowledge and Skills), it’s about assessing a learner’s  
 318 overall ability to do that work (the combination of TKS statements that it encompasses).  
 319 Competencies offer an opportunity to increase alignment and coordination between employers,  
 320 learners, and education and training providers (see Figure 1: NICE Competencies Stakeholders).



**Figure 1: NICE Competencies Stakeholders**

321 Competencies offer a higher-level perspective on cybersecurity work, allowing organizations to  
 322 bring together various TKS statements into an overarching group that defines a broad need. As  
 323 such, they allow organizations to, for instance, develop position descriptions without having to

---

alignment review.

324 delve into the details of the statements they comprise. In addition, Competencies are flexible,  
325 allowing the inclusion or removal of individual TKS statements over time in response to shifting  
326 needs in a changing cybersecurity ecosystem. It is recognized that additional work is required to  
327 review and update existing TKS statements in order to better align them to the identified list of  
328 competencies. That work is ongoing and will be updated periodically.

### 329 **2.2.1 Developing Competency Statements**

330 The following guidelines are used for the development of Competencies as part of the NICE  
331 Framework.

- 332 1. **Competency Title:** The name of the competency; the title should clearly signal to all  
333 stakeholders the area that will be described.
- 334 2. **Competency Description:** The description should:
  - 335 a. **Begin with “This Competency describes a learner’s capabilities related to....”**  
336 Using the same standard language to introduce each description serves as a  
337 signpost for readers that it is a Competency description while focusing the  
338 competency onto the learner (as opposed, for instance, to a Work Role or Task) at  
339 the onset.
  - 340 b. **Define the Competency simply and clearly.** Anyone reading the description  
341 should be able to quickly and easily understand the scope and meaning of the  
342 competency.
  - 343 c. **Reflect content from TKS statements.** The description may echo language from  
344 Task, Skill, or Knowledge statements that are associated with the Competency,  
345 though it should not wholly duplicate that language.
  - 346 d. **Balance specificity with broad application.** A goal of a NICE Framework  
347 Competency is to provide flexibility of application; the description should be  
348 detailed enough to clearly define its scope and meaning, but not so narrow as to  
349 restrict use by multiple stakeholders or time-date the competency (e.g., by  
350 referencing a particular computer program or coding language).
  - 351 e. **Omit unnecessary qualifiers.** Qualifiers (e.g., "Thorough Knowledge,"  
352 "Considerable Skill," or "Basic Understanding") and other indications of  
353 proficiency level should not be included in the Competency description.
- 354 3. **Associated TKS Statements:** Each Competency will be associated with a defined group  
355 of NICE Framework Task, Skill, and/or Knowledge statements that provide a more  
356 detailed view of the Competency. Note that individual statements may be associated with  
357 more than one Competency.

## 358 2.2.2 Example uses

359 The NICE Framework enables rapid adaptation to change while accounting for organizations’  
360 unique operating contexts. At the same time, by establishing common language and approach, a  
361 consistent exchange of cybersecurity workforce information is possible across an organization,  
362 among multiple organizations, and sector-wide. The Competencies extend the NICE Framework  
363 attributes of agility, flexibility, interoperability, and modularity, which is reflected in the multiple  
364 ways that they could be applied by its various stakeholders. There’s no one-size-fits-all: they can  
365 be used with a variety of assessment methods and, because of the way that Competencies tie in  
366 with the core NICE Framework building blocks, they can be used in parts or as a whole.

367 NICE Competencies provide users with a basis for building integrated human resource  
368 management systems that use a common set of Competencies to structure job design,  
369 recruitment, selection, performance management, training, and career development so that  
370 employees receive a consistent message about the factors on which they are selected, trained, and  
371 evaluated.

### 372 2.2.2.1 Employer Perspective

373 From an employer perspective, some ways Competencies can be used to:

- 374 • **Describe a given position:** For instance, position descriptions can refer to defined  
375 Competencies when developing a job description or defining a new role for their  
376 organization.
- 377 • **Track workforce capabilities:** Defined Competencies can be used to broadly describe  
378 and track an organization’s cybersecurity workforce knowledge and skills, or an  
379 employer might look at a grouping of tasks and define a Competency from that group for  
380 their unique needs.
- 381 • **Specify team requirements:** At times, individual tasks a team might need to complete  
382 may be unknown at the onset. In these cases, the Competencies necessary to solve the  
383 challenge can be used to identify team members, who will then determine the specific  
384 work to be done.
- 385 • **Assess individual learner capabilities:** Learners can be assessed against Competencies  
386 at various or multiple stages, including as part of an interview, a work-based learning  
387 evaluation, a promotion process, or career development.

### 388 2.2.2.2 Education, Training, or Credential Provider Perspective

389 From an education, training, or credential provider perspective, some applications might include:

- 390 • **In program development:** Providers could use a set of Competencies to develop a  
391 learning program—bundling together related competencies or perhaps differentiating  
392 levels of proficiency within a Competency.

393 • **In course development:** Instructors might look at the most important Knowledge and  
394 Skill statements reflected in a Competency to focus on teaching those.

395 • **In student assessment:** Providers could use Tasks in a Competency to assess whether  
396 learners have achieved the knowledge and skills needed in that area in order to issue a  
397 credential.

### 398 2.2.2.3 Learner Perspective

399 Finally, from the learner's perspective, Competencies can be used at various stages and in  
400 various ways, such as to:

401 • **Assess one's abilities:** For example, to determine if one can complete defined tasks in a  
402 Competency.

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

405 • **Learn about a defined area of expertise:** Competencies can offer a bird's eye view for  
406 anyone interested cybersecurity to help them discover more defined areas, as well as  
407 connect a learner to the details via the associated TKS statements.

408 • **Understand an organization's workforce needs:** For learners who are looking for a  
409 new job, in a current position but may want to make a shift, or want to plan their career  
410 path, Competencies can give insight into an organization's cybersecurity workforce.

411

412 **References**

- 413 [1] Petersen R, Santos D, Wetzel K, Smith M, Witte G (2020) Workforce Framework for  
414 Cybersecurity (NICE Framework). (National Institute of Standards and Technology,  
415 Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1.  
416 <https://doi.org/10.6028/NIST.SP.800-181r1>
- 417 [2] National Institute of Standards and Technology (2021) *NICE Framework Resource*  
418 *Center*. Available at <https://www.nist.gov/itl/applied-cybersecurity/nice/resources>
- 419 [3] Berry, J (2011) Competency Model for Cybersecurity. (The White House, Washington,  
420 DC), U.S. Office of Personnel Management Memorandum, February 16, 2011. Available  
421 at <https://www.chcoc.gov/content/competency-model-cybersecurity>
- 422



423 **Appendix A—Acronyms**

424 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

425

426 **Appendix B—Glossary**

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

430 **Competency** A mechanism for organizations to assess learners.

431 **Knowledge** A retrievable set of concepts within memory.

432 **Skill** The capacity to perform an observable action.

433 **Task** An activity that is directed toward the achievement of organizational  
434 objectives.

435 **Work Role** A way of describing a grouping of work for which someone is responsible or  
436 accountable.