

3 **Workforce Framework**  
4 **for Cybersecurity**  
5 **(NICE Framework)**

---

6  
7 Rodney Petersen  
8 Danielle Santos  
9 Matthew Smith  
10 Greg Witte

11  
12  
13  
14 This publication is available free of charge from:  
15 <https://doi.org/10.6028/NIST.SP.800-181r1-draft>  
16  
17  
18  
19

20 **Draft NIST Special Publication 800-181**  
21 **Revision 1**

22 **Workforce Framework**  
23 **for Cybersecurity**  
24 **(NICE Framework)**

26 Rodney Petersen (Director)  
27 Danielle Santos (Program Manager)  
28 *National Initiative for Cybersecurity Education (NICE)*  
29 *Applied Cybersecurity Division*  
30 *Information Technology Laboratory*

31  
32 Matthew Smith  
33 Greg Witte  
34 *Huntington Ingalls Industries*  
35 *Annapolis Junction, MD*

36  
37  
38 This publication is available free of charge from:  
39 <https://doi.org/10.6028/NIST.SP.800-181r1-draft>

40  
41 July 2020  
42



43  
44  
45  
46 U.S. Department of Commerce  
47 *Wilbur L. Ross, Jr., Secretary*

48  
49 National Institute of Standards and Technology  
50 *Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology*

51

## Authority

52 This publication has been developed by NIST in accordance with its statutory responsibilities under the  
53 Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law  
54 (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including  
55 minimum requirements for federal information systems, but such standards and guidelines shall not apply  
56 to national security systems without the express approval of appropriate federal officials exercising policy  
57 authority over such systems. This guideline is consistent with the requirements of the Office of Management  
58 and Budget (OMB) Circular A-130.

59 Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and  
60 binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these  
61 guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce,  
62 Director of the OMB, or any other federal official. This publication may be used by nongovernmental  
63 organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would,  
64 however, be appreciated by NIST.

65 National Institute of Standards and Technology Special Publication 800-181  
66 Natl. Inst. Stand. Technol. Spec. Publ. 800-181 Rev. 1, 23 pages (July 2020)  
67 CODEN: NSPUE2

68 This publication is available free of charge from:  
69 <https://doi.org/10.6028/NIST.SP.800-181r1-draft>

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

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

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

83 **Public comment period: July 15, 2020 through August 28, 2020**

84 Email: [NICEFramework@nist.gov](mailto:NICEFramework@nist.gov)

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

86

## Reports on Computer Systems Technology

87 The Information Technology Laboratory (ITL) at the National Institute of Standards and  
88 Technology (NIST) promotes the U.S. economy and public welfare by providing technical  
89 leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test  
90 methods, reference data, proof of concept implementations, and technical analyses to advance the  
91 development and productive use of information technology. ITL's responsibilities include the  
92 development of management, administrative, technical, and physical standards and guidelines for  
93 the cost-effective security and privacy of other than national security-related information in federal  
94 information systems. The Special Publication 800-series reports on ITL's research, guidelines, and  
95 outreach efforts in information system security, and its collaborative activities with industry,  
96 government, and academic organizations.

97

### Abstract

98 This publication describes the Workforce Framework for Cybersecurity (NICE Framework), a  
99 fundamental reference for describing and sharing information about cybersecurity work. It  
100 expresses that work as Task statements and defines Work Roles that perform those tasks. It also  
101 describes Knowledge and Skill statements that provide the foundation for lifelong learners to  
102 accomplish tasks. Additionally, Competencies are introduced as a way to further describe  
103 learners (employees, job seekers, and students) by grouping sets of knowledge and skills. As a  
104 common, consistent lexicon that categorizes and describes cybersecurity work, the NICE  
105 Framework improves communication about how to identify, recruit, develop, and retain  
106 cybersecurity talent. The NICE Framework is a reference source from which organizations or  
107 sectors can develop additional publications or tools that meet their needs to define or provide  
108 guidance on different aspects of cybersecurity education, training, and workforce development.

109

### Keywords

110 Competency; cybersecurity; cyberspace; education; knowledge; role; security; skill; task; team;  
111 training; workforce; work role.

112

### Supplemental Content

113 A Reference Spreadsheet for the original NICE Framework is available at  
114 <https://www.nist.gov/file/372581>.

115

116

## Call for Patent Claims

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

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

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

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

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

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

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

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

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

142

143

## Document Conventions

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

152

**Acknowledgments**

153 The NICE Framework was developed by a Core Authoring Team that includes representatives  
154 from numerous departments and agencies in the United States federal government. The National  
155 Institute of Standards and Technology wishes to acknowledge and thank these team members  
156 whose dedicated efforts contributed significantly to the publication:

157 William Newhouse, National Institute of Standards and Technology  
158 Pam Frugoli, Department of Labor  
159 Lisa Dorr, Department of Homeland Security  
160 Kenneth Vrooman, Cybersecurity and Infrastructure Security Agency  
161 Bobbie Sanders, Department of Defense  
162 Matt Isnor, Department of Defense  
163 Stephanie Shively, Department of Defense  
164 Ryan Farr, Department of Defense

165 The authors and the Core Authoring Team gratefully acknowledge and appreciate the significant  
166 contributions from individuals and organizations in the public and private sectors whose  
167 thoughtful and constructive comments improved the overall quality, thoroughness, and  
168 usefulness of this publication. Additionally, the authors would like to acknowledge the work of  
169 the authors of the original SP 800-181 Cybersecurity Workforce Framework: William Newhouse  
170 of NIST; Stephanie Keith of the U.S. Department of Defense; and Benjamin Scribner of the U.S.  
171 Department of Homeland Security.

172 The first NICE Framework was posted for public comment in September 2012 and published as  
173 final in April 2013 as the National Cybersecurity Workforce Framework version 1.0 [1]. The  
174 authors recognize Dr. Jane Homeyer, Anne Quigley, Rex Min, Noel Kyle, Maya Yankelevich,  
175 and Peggy Maxson for leading its development, along with Montana Williams and Roy Burgess  
176 for their leadership in the development of National Cybersecurity Workforce Framework version  
177 2.0 which was posted in April 2014 [2].

178

**Note to Reviewers**

179 Welcome to the National Initiative for Cybersecurity (NICE) Workforce Framework for  
180 Cybersecurity (NICE Framework), Revision 1 draft. The NICE Program Office staff have  
181 received significant feedback from the community including through many responses to a recent  
182 Request for Comments. In light of that feedback and the fast-paced and connected ecosystem of  
183 cybersecurity, the authoring team decided to adopt and promote attributes of agility, flexibility,  
184 interoperability, and modularity. These attributes led to a refactoring of the NICE Framework to  
185 provide a streamlined approach for managing the workforce. Below is a summary of changes:

- 186 ● Organizing constructs in Revision 1 have been simplified by deprecating Categories (e.g.,  
187 securely provision, oversee and govern, protect and defend, analyze, etc.) and Specialty  
188 Areas (e.g., incident response, threat analysis, cybersecurity management, etc.). In order  
189 to simplify an approach that offers agility, flexibility, interoperability, and modularity for  
190 organizations, Revision 1 presents a streamlined set of “building blocks” comprised of  
191 Knowledge, Skills, and Tasks as well as Work Roles. Organizations that find value in the  
192 former Categories and Specialty areas can create “Teams” around those concepts and  
193 align them with this version of the NICE Framework (See Section 3.4).
- 194 ● The relationships among Knowledge, Skill, and Abilities and Tasks have changed. Skill  
195 and Ability statements from the previous version have been refactored for simplicity into  
196 Skill statements which focus on the action of the learner. Knowledge and Skill statements  
197 can then associate with Task Statements.
- 198 ● The “lists” of Knowledge, Skill, Task, and Work Roles have been removed from the  
199 document. This helps to separate the maintenance of the NICE Framework from the  
200 content itself. In support of agility and flexibility, the Task, Knowledge, and Skill (TKS)  
201 Statements and list of Work Roles are currently under development. NICE expects to  
202 provide an additional resource in the future, possibly to include some options for  
203 grouping of Work Roles, and will request public comment at that time.
- 204 ● Many of the resources (e.g., the supplemental spreadsheet, KSAs, Work Roles, Online  
205 Informative Reference catalog entries) from the original NICE Cybersecurity Workforce  
206 Framework are being updated based on feedback received and other lessons learned. In  
207 support of interoperability and modularity, forthcoming work will update these  
208 statements to match the final definitions of TKS Statements noted here.

209 Questions to the Reviewer:

- 210 ● Users may want “NICE approved” TKS, Work Roles, and Competencies. What is a  
211 recommended way to develop and manage such a list? Does it make sense that NICE  
212 could prescribe aspects of the NICE Framework without knowing an organization’s  
213 structure and mission?
- 214 ● The current definition of Competency within the NICE Framework is one of many used  
215 in the community. Does this definition and formulation help clarify and specify  
216 workforce management?
- 217 ● The current draft does not address “proficiency” in a Work Role (e.g., Entry-,  
218 Intermediate-, or Advanced-Level). Is this concept needed in the NICE Framework or  
219 best left to users or to be explored in a corresponding publication (e.g., NISTIR)?

## 220 **Executive Summary**

221 Each of us—individually and organizationally—performs important work that provides a  
222 contribution to society. However, it is often difficult, to clearly describe the work that one is  
223 performing or desires to accomplish. Information and technology, including many evolving types  
224 of operational technology, grow increasingly complex and interconnected every day. The  
225 National Initiative for Cybersecurity Education (NICE) recognizes that the participants in that  
226 evolution are lifelong learners, from their first day in a classroom to long after their retirement  
227 party, and that there is a segment of learners that are responsible for maintaining confidentiality,  
228 integrity, and availability objectives. In this publication, that segment is referenced as the  
229 cybersecurity workforce and the tasks that they perform are referenced as the cybersecurity  
230 work. There is value in describing that work with precision when recruiting, hiring, developing,  
231 and retaining employees or contractors.

232 The NICE Framework has been developed by to help provide a reference taxonomy of the  
233 cybersecurity work and of the individuals who carry out that work. The NICE Framework  
234 supports the NICE mission to energize and promote a robust network and an ecosystem of  
235 cybersecurity education, training, and workforce development. The NICE Framework provides a  
236 set of building blocks for describing the tasks, knowledge, and skills that are needed to perform  
237 cybersecurity work performed by individuals and teams. Through these building blocks, the  
238 NICE Framework enables organizations to develop their workforces to perform cybersecurity  
239 work and helps learners to explore cybersecurity work and to connect with initiatives develop  
240 their knowledge and skills. This development, in turn, benefits employers and employees  
241 through the identification of career pathways that document how to prepare for cybersecurity  
242 work using the data of TKS Statements bundled into Work Roles and Competencies.

243 There are numerous benefits to both individuals and organizational entities from applying such a  
244 framework. The use of common terms and language helps to organize and communicate the  
245 work to be done and the attributes of those that are qualified to perform that work. In this way  
246 the NICE Framework helps to simplify communications and provide focus on the tasks at hand,  
247 such as for cybersecurity work to be accomplished. Use of the NICE Framework improves  
248 clarity and consistency at all organizational levels—from an individual to a technology system to  
249 a program, organization, sector, state, or nation.



250 **Table of Contents**

251 **Executive Summary ..... vi**

252 **1 Background ..... 1**

253 1.1 Attributes of the NICE Framework ..... 2

254 1.2 Purpose and Applicability..... 2

255 1.3 Audience..... 3

256 1.4 Organization of this Publication ..... 3

257 **2 NICE Framework Components..... 4**

258 2.1 Task Statements ..... 4

259 2.2 Knowledge Statements ..... 4

260 2.3 Skill Statements ..... 5

261 **3 Using the NICE Framework Building Blocks ..... 6**

262 3.1 Applying the NICE Framework..... 6

263 3.1.1 Using Existing TKS Statements..... 6

264 3.1.2 Creating New TKS Statements..... 6

265 3.2 Work Roles ..... 6

266 3.2.1 Using Existing Work Roles ..... 7

267 3.2.2 Creating a New Work Role ..... 7

268 3.3 Competencies ..... 7

269 3.3.1 Using Existing Competencies ..... 8

270 3.3.2 Creating New Competencies ..... 8

271 3.4 Teams ..... 9

272 3.4.1 Building Teams with Work Roles ..... 9

273 3.4.2 Building Teams with Competencies..... 10

274 **4 Conclusion ..... 12**

275 **References ..... 13**

276

277 **Appendix A— Acronyms ..... 14**

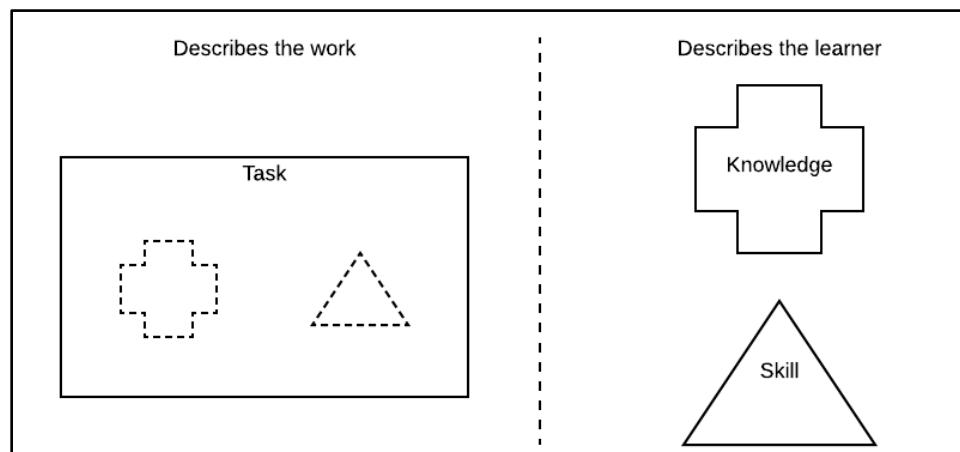
278

279 **1 Background**

280 Technology continues to evolve at an ever-increasing pace. Specifically, the technology which  
 281 facilitates the ability to access and process information quickly and efficiently is dramatically  
 282 changing. The work required to build, secure, and implement these data, networks, and systems  
 283 increases in complexity. Furthermore, describing this work and those who can perform the work  
 284 remains a challenge. Compounding this problem, organizations use varying and self-created  
 285 methods to help solve this definition challenge. Thus, communication among organizations  
 286 regarding security initiatives and the people who perform them remains difficult.

287 The Workforce Framework for Cybersecurity (NICE Framework) helps organizations overcome  
 288 the barrier of describing their workforce to multiple stakeholders by presenting a building block  
 289 approach. Through the use of conceptual building blocks, the NICE Framework presents a  
 290 common language for organizations to use internally and with others. This approach allows  
 291 organizations to tailor and implement the NICE Framework to their unique operating context.  
 292 Furthermore, by creating a common language the NICE Framework lowers the barrier to entry  
 293 for organizations seeking to enter and interoperate with other organizations.

294 Figure 1, below, depicts a high-level view of the NICE Framework. The main building blocks of  
 295 the NICE Framework are Tasks, Knowledge, Skills (explained in Section 2) that are shown  
 296 alongside the concepts they describe. Figure 1 shows that there are two main types of concepts  
 297 being described: “the work” and “the learner.” The NICE Framework attempts to describe both  
 298 of these in generic terms that can be applied to all organizations.



299  
300 **Figure 1 - NICE Framework Approach**

301 The “work” is what an organization executes on a daily basis. Every organization executes  
 302 common Tasks as well as some context-unique Tasks. For example, every organization has some  
 303 form of management tasks, whereas only some organizations have Tasks to “deploy bulk energy  
 304 systems securely.” The NICE Framework provides organizations a way to describe their work  
 305 through Task statements that group supporting Knowledge and Skill statements.

306 The “learner” is the person who carries out the Task. It is important to remember that all people  
 307 are constantly learning and achieving objectives. These objectives can be better management  
 308 skills, more in-depth technical knowledge, or other Knowledge or Skills. Therefore, “learners”

309 can be any part of the learning lifecycle such as students, current employees, or job seekers. The  
310 NICE Framework provides organizations a way to describe “learners” by associating Knowledge  
311 and Skill statements that enable task completion.

312 By describing both the “work” and the “learner,” the NICE Framework provides organizations a  
313 common language to describe their cybersecurity work. Furthermore, the NICE Framework  
314 provides a mechanism to communicate across organizations at a peer level, sector level, national  
315 level, or international level using the same building blocks. This communication can drive  
316 innovative solutions to common challenges, lower barriers to entry for new organizations and  
317 individuals, and facilitate workforce mobility.

## 318 **1.1 Attributes of the NICE Framework**

319 The NICE Framework is a reference resource for those seeking to describe the cybersecurity  
320 work their organization does, the people that will carry out the work, and the ongoing learning  
321 that will be needed. The nature of the work, and consequently the workforce, can be described  
322 using the building blocks presented in the following sections. These building blocks incorporate  
323 the following attributes:

- 324 ● **Agility**—People, processes, and technology mature and must adapt to change. Therefore,  
325 the NICE Framework enables organizations to keep pace with a constantly evolving  
326 ecosystem.
- 327 ● **Flexibility**—While every organization faces similar challenges, there is no one-size-fits-  
328 all solution to those common challenges. Therefore, the NICE Framework enables  
329 organizations to account for the organization’s unique operating context.
- 330 ● **Interoperability**—While every solution to common challenges is unique, those solutions  
331 must agree upon consistent use of terms. Therefore, the NICE Framework enables  
332 organizations to exchange workforce information using a common language.
- 333 ● **Modularity**—While cybersecurity risk remains the basis of this document, there are  
334 other risks that organizations must manage within the enterprise. Therefore, the NICE  
335 Framework enables organizations to communicate about other types of workforces within  
336 an enterprise and across organizations or sectors (e.g., Privacy, Artificial Intelligence).

## 337 **1.2 Purpose and Applicability**

338 Organizations manage many different business functions such as operations, finance, legal,  
339 human resources, etc., as part of their overall enterprise. Each of these business functions has  
340 associated risks. As technology has become an enabling factor in managing an enterprise, the  
341 risks associated with cybersecurity have also become more prominent. The NICE Framework  
342 assists organizations with managing cybersecurity risks by providing a way to discuss the  
343 “work” and “learners” associated with cybersecurity. These cybersecurity risks are an important  
344 input into enterprise risk decisions, as described in NIST Interagency Report 8286, *Integrating*  
345 *Cybersecurity and Enterprise Risk Management (ERM)*. [3]

346 This document serves as a potential guideline for other business functions that are considering  
347 the creation of Workforce Frameworks. By using the same building blocks across various  
348 business functions, organizations can increase efficiency. Therefore, any organization can  
349 leverage this document.

### 350 **1.3 Audience**

351 The topic of managing a workforce for cybersecurity involves many different types of positions,  
352 as well as many different types of organizations. The audience of this document is: public sector  
353 agencies, private companies, academia, hiring managers, line managers, workforce planners,  
354 curriculum developers, credential providers, recruiters, and all learners.

### 355 **1.4 Organization of this Publication**

356 The remainder of this special publication is organized as follows:

- 357 • Chapter 2 defines the building block components (Tasks, Knowledge, and Skills) of the  
358 NICE Framework,
- 359 • Chapter 3 describes common uses of the NICE Framework,
- 360 • A list of References to publications related to this publication is included after Chapter 3,  
361 and
- 362 • Appendix A provides a list of abbreviations and acronyms used in this publication.

## 2 NICE Framework Components

The Workforce Framework for Cybersecurity (NICE Framework) is built upon a set of discrete components that describe the work to be done (in the form of Tasks) and the learners who perform that work (through Knowledge and Skills).

### 2.1 Task Statements

Task: an activity that is directed toward the achievement of objectives.

As depicted in Figure 1, Task statements describe the work, and Skill statements describe the learner. Therefore, it is important to distinguish the language used between Skill statements and Task statements. Task statements should focus on the organizational language and communication patterns that provide value to the organization. These statements are designed to describe work to be done and should be aligned with the context of the organization.

Tasks describe work to be completed. The objectives of this work can be business objectives, technology objectives, or mission objectives. Task statements should be straightforward. While the work encompassed within a Task statement may have many steps, as with the example below, the statement itself is easy to read and understand.

A Task statement begins with the activity being executed.

Example: **Troubleshoot** system hardware and software.

A Task statement does not contain the objective within the Task statement.

Example: Conduct interactive training exercises ~~to create an effective learning environment.~~

As Figure 1 depicts, Tasks are related to Knowledge and Skill (K&S) statements. A learner will demonstrate that they possess the knowledge and skill to complete a task or be challenged to gain the knowledge and learn the skill to prepare to complete the task. The complexity within a Task is explained by the associated K&Ss. In the troubleshooting example above, in order to effectively troubleshoot any piece of software or hardware, the learner should be familiar with and understand the related Knowledge statements. The same can be said for Skill statements.

### 2.2 Knowledge Statements

Knowledge: a retrievable set of concepts within memory.

Knowledge statements can be foundational.

Example: Knowledge of cyberspace threats and vulnerabilities.

Knowledge statements can be specific.

Example: Knowledge of vulnerability information dissemination sources (e.g., vendor alerts, government advisories, product literature errata, and sector bulletins).

396 Knowledge statements relate to Task statements in that only with the understanding described by  
397 the Knowledge statement will the learner be able to complete the Task. There may be multiple  
398 Knowledge statements that are needed to complete a given Task. Likewise, one Knowledge  
399 statement may be used to complete many different Tasks.

### 400 **2.3 Skill Statements**

401 Skill: the capacity to perform an observable action.

402 Skill statements can be straightforward.

403       Example: Recognize the alerts of an Intrusion Detection System

404 Skill statements can be complex.

405       Example: Generate a hypothesis as to how a threat actor circumvented the Intrusion  
406       Detection System.

407 Skill statements relate to Task statements in that a learner is demonstrating skills in performing  
408 tasks. A learner who is not able to demonstrate the described skill would not be able to complete  
409 the Task that relies on that skill. There may be multiple Skill statements that are needed to  
410 complete a given Task. Likewise, exercising a skill may be used to complete more than one  
411 Task.

412 As depicted in Figure 1, Skill statements describe what the learner can do, and Task statements  
413 describe the work to be done. Therefore, it is important to separate the language used between  
414 Skill statements and Task statements. Skill statements should use language such as that which is  
415 outlined in Bloom's Taxonomy (Revised) because it facilitates observability and assessment of  
416 the learner. [4]

## 417 **3 Using the NICE Framework Building Blocks**

### 418 **3.1 Applying the NICE Framework**

419 Notably, while the Workforce Framework for Cybersecurity (NICE Framework) is intended to  
420 provide a common set of building blocks from which many can draw, many organizations will  
421 find the need to tailor the model to align more closely with their unique context. For example, a  
422 manufacturer may have sector or organization-specific tasks that are not described in the NICE  
423 Framework. Others may find that the Tasks are applicable but need to adjust or develop specific  
424 K&S statements that increase the likelihood that the tasks can be completed as defined by the  
425 unique context of the organization.

#### 426 **3.1.1 Using Existing TKS Statements**

427 Each Knowledge and Skill statement is intended to support various tasks, and the Task  
428 statements may support one or more Work Roles. Although a Task statement may have a  
429 predetermined set of associated K&S statements, users may include other existing Ks and Ss to  
430 tailor Tasks for their unique context. Similarly, a user may wish to draw from the listed Tasks  
431 and add additional ones to those supporting a Work Role. The current set of NICE Framework  
432 components is available from the NICE Framework Resource Center.

433 Users are cautioned against internally modifying the text in an existing NICE Framework  
434 Component. The statements are intended to support interoperability, so changing their content  
435 may result in subsequent misalignment. If different wording is needed in a TKS statement, a new  
436 statement can be created as described below.

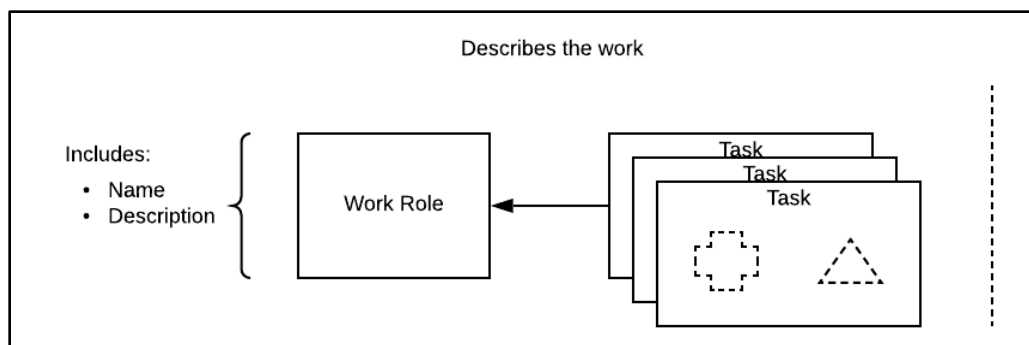
#### 437 **3.1.2 Creating New TKS Statements**

438 Users may also create new Task, Knowledge, or Skill statements to help tailor the use of the  
439 NICE Framework for their unique context. Such additional statements will help support clear and  
440 consistent internal discussions regarding learners and their work activities. Any internally  
441 developed statements should follow the guidance to be provided in the future.

### 442 **3.2 Work Roles**

443 A key building block of the NICE Framework is described by Work Roles. Work Roles are a  
444 way of describing a grouping of work for which someone is responsible or accountable. Each  
445 Work Role is associated with a given set of Task statements, thereby describing a “work-  
446 centered” view of workforce management.

447 While previous workforce frameworks also associated Work Roles with knowledge, skill, and  
448 ability specifications, the NICE Framework encourages a more agile approach through Tasks.  
449 Work Roles are composed of Task statements that constitute the work to be done; Task  
450 statements, as described above, include associated Knowledge and Skill statements that represent  
451 learners’ potential to perform those tasks. This transitive approach, illustrated in Figure 2,  
452 supports flexibility and simplifies communication.



453

454

**Figure 2 - Work Roles' Relationship to Task Statements**

455 Work Role names are not synonymous with job titles, though some Work Roles may coincide  
 456 with a job title. Similarly, a single Work Role (e.g., Software Developer) may apply to those  
 457 with many varying job titles (e.g., software engineer, coder, application developer.) This method  
 458 supports improved modularity and illustrates the fact that all in the workforce perform numerous  
 459 tasks in various roles, regardless of their job titles. Similarly, the NICE Framework does not  
 460 provide for attribution of adjectives such as Entry-, Intermediate-, or Advanced-level. Such  
 461 attributes, and those regarding the proficiency with which a learner performs tasks, are left to  
 462 other models or resources.

### 463 3.2.1 Using Existing Work Roles

464 Each Work Role is intended to support the achievement of objectives through Tasks. Although a  
 465 Work Role may have a predetermined set of associated Tasks, users may include other existing  
 466 Tasks to tailor Work Roles for their unique context. Similarly, a user may wish to draw from the  
 467 listed Work Roles or add additional ones to support additional objectives. The current set of  
 468 NICE Framework components is available from the NICE Framework Resource Center.

469 Users are cautioned against internally modifying the text in an existing NICE Framework  
 470 Component. The Work Roles are intended to support interoperability so changing their content  
 471 may result in subsequent misalignment. If different wording is needed, a new Work Role can be  
 472 created as described below.

### 473 3.2.2 Creating a New Work Role

474 Users may also create new Work Roles to help tailor the use of the NICE Framework for their  
 475 unique context. Such additional Work Roles will help support clear and consistent internal  
 476 discussions regarding the cybersecurity work. Any internally developed Work Roles should  
 477 follow the guidance to be provided in the future.

## 478 3.3 Competencies

479 Competency: an observable group of related Knowledge and Skills statements.

480 Competencies are a way to further describe learners. Figure 3 depicts a grouping of K&S  
 481 statements. By grouping sets of Knowledge and Skills, Competencies allow learners to  
 482 succinctly communicate and effectively demonstrate that they have the requisite Knowledge and



483 Skills to perform cybersecurity work. The underlying Knowledge and Skills do not change;  
 484 however, the grouping provided by Competencies provides a streamlined view of a learner. As  
 485 such, Competencies are a “learner-centered” view of workforce management. The flexibility of  
 486 Competencies allows organizations and learners to adapt to the changing cybersecurity  
 487 ecosystem.

488

### 489 3.3.1 Using Existing Competencies

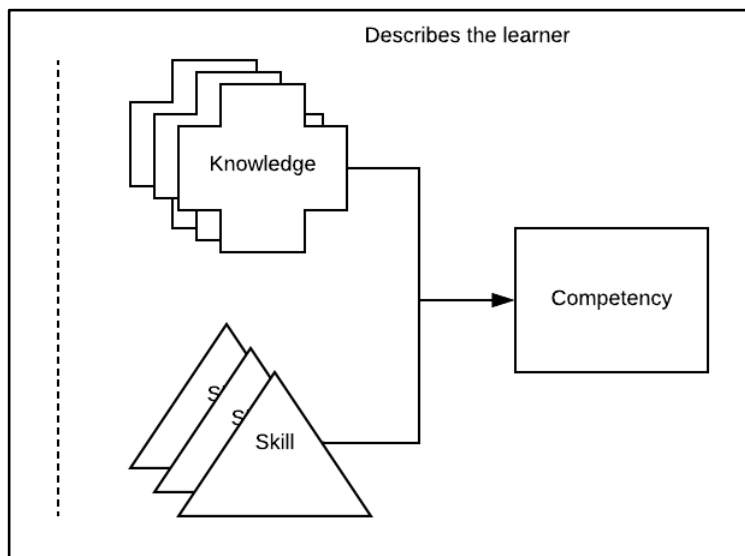


Figure 3 - How Competencies Relate to Knowledge and Skills Statements

490 Organizations have provided examples of Competencies within their industries. NIST is  
 491 developing a set of these in the forthcoming Draft Special Publication (SP) 800-16 Revision 2,  
 492 *Cybersecurity Role Profiles for Training*. [5] These concepts can be adapted to fit within the  
 493 Competency component provided above. By mapping the Competency into its constituent K&S  
 494 statements, the Competency is then aligned to the NICE Framework.

495 As mentioned in section 3.1.2, it is possible to tailor the NICE Framework. Existing  
 496 Competencies may highlight the need for new K&S statements. By creating these new K&S  
 497 statements, the user of the NICE Framework can tailor the NICE Framework to meet their  
 498 unique requirements. Using the Competency concept allows organizations to practice  
 499 interoperability between frameworks by using a common language and building blocks.

### 500 3.3.2 Creating New Competencies

501 Some organizations may need to describe a competency for the specific context of their  
 502 cybersecurity work. The NICE Framework, developed with the principle of Agility, allows  
 503 organizations to describe a competency to meet a changing cybersecurity ecosystem. Creating or  
 504 identifying relevant competencies is a flexibility offered by mapping Ks and Ss that are valued  
 505 by subject matter experts who wish to use a competency to support conversations between  
 506 managers and employees, for example.

507 Additionally, if an organization wanted to create a Competency for Data Analysis, it could look  
508 like the following:

509 **Table 1 - Creating a Data Analysis Competency**

<b>Competency Name:</b> Data Analysis	
<b>Competency Description:</b> The collecting, synthesizing, or analyzing qualitative and quantitative data and information from a variety of sources to reach a decision, make a recommendation, and/or compile reports, briefings, executive summaries, and other correspondence.	
<b>Knowledge Statements</b>	<b>Skill Statements</b>
Knowledge of statistical primitives	Evaluates information for reliability, validity, and relevance
Knowledge of data structures	Analyzes meaning across data sets
Knowledge of analytic tools and techniques for language, voice, and/or graphic material.	Performs sensitivity analysis

510

511 Table 1 demonstrates a way of creating Competencies. The example presented in Table 1 is  
512 informative and provides a starting point for building a Competency. A fully detailed  
513 Competency of Data Analysis would be much larger. The Data Analysis Competency has a name  
514 and a description that quickly allows the learner or the organization allows the learner to identify  
515 a competency as one they possess or aspire to achieve. By enumerating the K&S statements  
516 within the Competency, the learner or the organization can specify the desired scope of the  
517 Competency.

## 518 **3.4 Teams**

519 Many organizations use teams to collectively tackle complex challenges by bringing together  
520 individuals with complementary skills and experience. By utilizing different resources and  
521 perspectives, teams allow organizations to manage risks holistically. Teams take advantage of  
522 each member's specialization of knowledge and processes to effectively distribute work.

### 523 **3.4.1 Building Teams with Work Roles**

524 Teams can be built from a work-centered approach using Work Roles. A work-centered  
525 approach to building teams allows organizations to define what types of Work Roles are  
526 appropriate for achieving objectives. Consequently, these Work Roles execute the Tasks needed  
527 to achieve the objectives. Since Work Roles are made up of Tasks, this approach to building  
528 teams starts with the work.

529

**Table 2 - Example of a Secure Software Development Team**

<b>Lifecycle Phase</b>	<b>Work Role</b>
Design	Security Architect
Build	Software Developer
Deploy	Network Operations Specialist
Operate	Customer Support Specialist
Maintain	Database Administrator
Decommission	Communications Specialist

530

531 Table 2, above, describes an example Secure Software Development team. Teams built using  
 532 Work Roles begin with the identification of the work which needs to be accomplished. Secure  
 533 software development has lifecycle phases designed to achieve objectives of security and quality  
 534 of software. These objectives are linked to Tasks, and thus, Work Roles. Table 2 is an  
 535 informative example and does not cover all Work Roles which may be present. For more  
 536 information, see NIST's Secure Software Development Framework. [6]

537

**Table 3 - Example of a Cybersecurity Team**

<b>Cybersecurity Framework Function</b>	<b>Work Role</b>
Identify	Risk Manager
Protect	Controls Assessor
Detect	Cyber Defense Analyst
Respond	Incident Responder
Recover	Communications Specialist

538

539 Table 3 describes an example Cybersecurity Team. Similar to the Secure Software Development  
 540 team, the example Cybersecurity team is built with a work-centered approach. By using the Core  
 541 of the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity  
 542 Framework), cybersecurity objectives are selected, Tasks are identified to achieve those  
 543 objectives, and Work Roles are selected to define the roles necessary to support those objectives.  
 544 Table 3 is an informative example and does not cover all Work Roles which may be present. For  
 545 more information, see NIST's Cybersecurity Framework. [7]

### 546 **3.4.2 Building Teams with Competencies**

547 Teams can also be built using Competencies through a learner-centered approach. This approach  
 548 to building teams recognizes that the individual Tasks may be unknown, but the types of  
 549 Competencies needed to solve the challenge are known. Therefore, teams can be built by using a  
 550 group of Competencies to identify learners who might help with work in the future. Since  
 551 Competencies are made up of K&S statements, this approach to building teams starts with the  
 552 learners.

553 For example, a defensive cybersecurity team that uses its skills to imitate adversaries' attack  
554 techniques (i.e., a "Red Team") may be composed of the following competencies:

- 555 • Competency: Engagement Planning
- 556 • Competency: Rules of Engagement
- 557 • Competency: Pen Testing
- 558 • Competency: Data Collection
- 559 • Competency: Vulnerability Exploitation

**4 Conclusion**

561 Through the application of the building block approach described by the NICE Framework, users  
562 can benefit from a consistent method for organizing and communicating the work to be done  
563 (e.g., through Task statements) and the knowledge and skills of individual learners that support  
564 that work.

565 The ability to describe knowledge and skills is important to ensure a comprehensive  
566 understanding of the work and the workforce. The NICE Framework provides an extensible  
567 reference resource that can be applied and used by various organizations to describe the work to  
568 be performed in many areas. The benefits to these organizations support the NICE mission of  
569 energizing and promoting a robust ecosystem of cybersecurity education, training, and workforce  
570 development.

571 **References**

- [1] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 1.0*, <https://www.nist.gov/file/359276>
- [2] National Initiative for Cybersecurity Education, *National Cybersecurity Workforce Framework, ver. 2.0*, <https://www.nist.gov/file/359261>
- [3] Stine K, Quinn S, Witte G, Gardner RK (2020) Integrating Cybersecurity and Enterprise Risk Management (ERM). (National Institute of Standards and Technology, Gaithersburg, MD), Second Draft NIST Interagency or Internal Report (IR) 8286. <https://doi.org/10.6028/NIST.IR.8286-draft2>
- [4] Anderson LW (ed.), Krathwohl DR (ed.), Airasian PW, Cruikshank KA, Mayer RE, Pintrich PR, Raths J, Wittrock, MC (2001) *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives*. (Addison Wesley Longman, Inc., New York, NY).
- [5] Newhouse W, Sanchez-Cherry K, Williams C, Van Duyn L (Forthcoming) *Cybersecurity Role Profiles for Training*. (National Institute of Standards and Technology, Gaithersburg, MD), Draft NIST Special Publication (SP) 800-16, Rev. 2.
- [6] Dodson D, Souppaya M, Scarfone K (2020) *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper. <https://doi.org/10.6028/NIST.CSWP.04232020>
- [7] National Institute of Standards and Technology (2018) *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. (National Institute of Standards and Technology, Gaithersburg, MD). <https://doi.org/10.6028/NIST.CSWP.04162018>

572

**573 Appendix A—Acronyms**

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

ERM	Enterprise Risk Management
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
ITL	NIST Information Technology Laboratory
K&S	Knowledge and Skill statement(s)
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SSDF	Secure Software Development Framework
TKS	Task, Knowledge, and Skill statements

575