BUILDING A STRONG CYBERSECURITY PIPELINE
Cybersecurity and Infrastructure Security Agency (CISA)

**VISION**
Secure and resilient infrastructure for the American people.

**MISSION**
Lead the Nation’s efforts to understand and manage risk to our critical infrastructure.
### The Cybersecurity Workforce Challenge

<table>
<thead>
<tr>
<th>Globally</th>
<th>Domestically</th>
<th>Locally</th>
</tr>
</thead>
<tbody>
<tr>
<td>• According (ISC)², the <strong>global cyber workforce shortage</strong> is projected to reach <strong>1.8 million by 2022</strong>&lt;br&gt;• That’s more than <strong>1 new cyber expert needed every minute</strong>*&lt;br&gt;There are over <strong>300,000 vacant cyber jobs</strong> in the United States&lt;br&gt;</td>
<td></td>
<td>• There are over <strong>60,000 vacant jobs</strong> in the <strong>D.C. metro area</strong>&lt;br&gt;• The <strong>top openings are</strong>:&lt;br&gt;  • Cyber Security Engineer&lt;br&gt;  • Cyber Security Analyst&lt;br&gt;  • Network Engineer / Architect</td>
</tr>
</tbody>
</table>
The National Initiative for Cybersecurity Education (NICE) Framework provides a common language to describe cyber positions and helps define professional requirements in cyber.

To ensure a robust pipeline of qualified cybersecurity professionals meet the demands of cybersecurity need, academia, government, and private sector must work together. The Framework is the foundation on which to build curricula, training, and job/workforce structures.

Merge disparate efforts across the state to standardize the implementation of the NICE Framework. Standardization enables effective education objectives and knowledge units creating a cohesive education track. Position descriptions and professional development tied to the NICE Framework enables career progression and mobility within the cybersecurity field. Increased clarity and uniformity leads to better recruitment and retention across the state.
The Framework organizes the cyber workforce as outlined below:

**Categories (7)** – Groups of work that share major job functions

**Specialty Areas (33)** – Distinct areas of cyber work

**Work Roles (52)** – The most detailed groupings of cyber work
The Framework is the core of CISA Cybersecurity Education and Workforce Resources

- **K-12**: 17 K-12 courses—integrated across multiple disciplines to promote innovative learning
- **CAE/SFS**: Knowledge units mapped to Framework competencies results in greater likelihood of success in future work
- **PDs/workforce**: Suite of tools designed to increase efficiency and effective workforce planning and recruitment
- **Training**: Training courses mapped to Framework for easier professional development
- **National alignment**: Creates a standardized lexicon and understanding of work, competencies, and behavioral indicators
It’s all on NICCS™

The Nation’s One-stop-shop for Cybersecurity Careers and Studies!

✓ 30,000+ visitors per month
✓ 4,000+ courses in the NICCS Training Catalog mapped to the National Cybersecurity Workforce Framework
✓ 100+ links to cybersecurity resources
✓ 15+ tools for managers, including a Cybersecurity Workforce Development Toolkit

https://niccs.us-cert.gov/
Integrating Cybersecurity in the Classroom

Encourage cyber knowledge and interest early with FREE K-12 curricula…

Get on board:

- 17 year-long courses plus modular project-driven content mapped to the NICE Framework
- 2,400+ content hours
- 14,800+ teachers use the curricula impacting more than
- 2,200,000 students across the U.S.
- Workshops for teachers
- Cybersecurity Summer Camps

Download the free curricula: nicerc.org

- Integrate real world cyber scenarios into science, math, and liberal arts
- Teacher and master notes
- Quizzes, worksheets, assessments
- Student workbooks
- No cybersecurity training needed
Colleges and Scholarships

National Centers of Academic Excellence (CAE) in Cyber Defense (CD) offer cybersecurity-related degree programs designated by DHS and NSA.

Share information about the CyberCorps® Scholarship for Service (SFS) program with students interested in studying cybersecurity:

- Since 2011, 3,600 students have completed the program at 74 SFS schools.
- SFS graduates have been hired at over 140 government entities.

274 CAEs in 48 states, D.C., and Puerto Rico.
Workforce Development Toolkit and Tools

**PREPARE**
- Assess goals
- Evaluate readiness

**PLAN**
- Inventory workforce
- Ongoing workforce planning

**BUILD**
- Close skill gaps
- Recruit for key skills

**ADVANCE**
- Retain staff
- Provide continuous development

**TOOLS**
- Workforce Planning Capability Maturity Matrix (CMM)
- Cybersecurity Workforce Planning Diagnostics
- NICE Framework
- Workforce Mapping Tool
- Team Traits/ Interview Questions
- Recruitment Checklist
- PushButton PD™ Generator Tool
- Retention Tips by Level
- Career Path Template
- NICCS Training Catalog
Mapping Tool

Getting Started
Welcome to the NICE Cybersecurity Workforce Framework Mapping Tool!

This tool enables cyber managers and human capital professionals to enter information about cyber positions to understand how well their teams align to the NICE Cybersecurity Workforce Framework (NICE Framework). The NICE Framework is a collection of definitions describing cybersecurity work and the skills required to perform it. It is a national standard that helps organizations strengthen their cyber teams.

This tool takes the guesswork out of using the NICE Framework—simply answer questions about each cybersecurity-related position and the tool will show you how each aligns to the NICE Framework and what can be done to strengthen the team.

The tool will:
- Help you inventory your cybersecurity workforce and begin workforce planning
- Enable you to print out a report to use for workforce development
- Prepare to report OPM cybersecurity position coding ("CIPM Data Element" Requirements)
- Determine the skills and type of training your team needs
- See where your staff may be underutilized

Continue from previous session
Enter the Session ID from your previous session to continue from where you left off.

Enter Your Session ID
Submit

Job Description Framework Alignment
Complete the questionaire below to describe the position. Fields marked with an asterisk (*) are required.

Select the statements below that best describe this position's work at a high level (choose up to 3) *
- [ ] Analyze - Reviews and evaluates incoming cybersecurity information to determine its usefulness for intelligence.
- [ ] Collect and Operate - Responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
- [ ] Investigate - Responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence.
- [ ] Operate and Maintain - Responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security.
- [ ] Overseas and Govern - Provides leadership, management, direction, and/or development and advocacy so that all individuals and the organization may effectively conduct
- [ ] Protect and Defend - Responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks.
- [ ] Securely Provision - Concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development.

Select the statements below that most specifically describe the position's work (choose up to 3) *

Select all functional areas that apply
- [ ] Intelligence Community (IC)
- [ ] Law Enforcement (LE)
- [ ] Legal
- [ ] Acquisition, Procurement, Resource Management, Budgeting, or Finance
- [ ] Technical
- [ ] DOD/GOV/FO

Select all knowledge, skills, or abilities possessed by this position *

Number of Roles - 26
The NICCS Education and Training Catalog is a central location where cybersecurity professionals across the nation can find over 3,000 cybersecurity-related courses.

Visit: https://niccs.us-cert.gov/training/search
DHS offers free cybersecurity training for U.S. government employees and Veterans!

- Courses range from beginner to advanced levels
- 250,000+ registered users
- 40,000+ Veteran users (through our non-profit partner Hire Our Heroes™)
- Over 60 courses - and growing!
- All courses are mapped to the NICE Framework

Fedvte.usalearning.gov
Career paths are designed to support cyber professionals, their supervisors, and human capital professionals with a range of workforce related activities, as outlined below:

- Conducting workforce assessment & planning activities
- Creating position descriptions (PDs)
- Identifying current training needs & professional development opportunities
- Enhancing recruitment and retention initiatives
- Improving job satisfaction through rewarding & challenging career opportunities

Note: These career paths are meant to be a framework; and can be tailored to meet the needs of each individual agency’s workforce.
## Coming soon: Sample Career Path

### Competency Model & Career Path

**Cyber Workforce Developer and Manager**

**Primary:** Cyber Workforce Developer & Manager (751)

**Secondary:** Cyber Policy and Strategy Planner (752), Program Manager (801)

**Date:** April 2019

### 2. CAREER PATH – CYBER WORKFORCE MANAGER AND DEVELOPER

#### 2.1 Description

The Cyber Workforce Manager and Developer work role is primarily aligned to the OPM occupational series (GS-2210, Information Technology Management) and is engaged in multiple tasks, as described in Table 1. Cyber Workforce Manager and Developer can conceivably be hired into other OPM occupational series as illustrated in Table 1 below.

<table>
<thead>
<tr>
<th>Cyber Workforce Manager and Developer Work Role Overview</th>
<th>OPM Occupational Series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary: Cyber Workforce Developer and Manager</td>
<td>751, Cyber Workforce Developer and Manager</td>
</tr>
<tr>
<td>Secondary: Cyber Policy and Strategy Planner</td>
<td>752, Cyber Policy and Strategy Planner</td>
</tr>
<tr>
<td></td>
<td>801, Program Manager</td>
</tr>
<tr>
<td></td>
<td>711, Cyber Instructional Curriculum Developer</td>
</tr>
<tr>
<td></td>
<td>712, Cyber Instructor</td>
</tr>
<tr>
<td></td>
<td>417, Data Analyst</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO Council</td>
<td>Establishes and implements the vision, mission, goals, and owns the business case, plans and strategies for a program in alignment with the organizational mission</td>
</tr>
<tr>
<td>CHCO Council</td>
<td>Aligns the IT/Cybersecurity workforce needs and priorities of the organization to strategic and operational workforce planning and talent management efforts</td>
</tr>
<tr>
<td>CISO</td>
<td>Anticipates and responds to federal personnel management trends that will impact the IT/Cybersecurity workforce or planning/analytic activities by identifying policy/guidelines or programs to enhance workforce performance (e.g., monitoring metrics, notices, changes in regulations)</td>
</tr>
</tbody>
</table>
Coming soon: Sample Career Path

2.5 Proficiency Levels

Each competency has several proficiency levels that map to career levels within the work role (Table 4).

| Cyber Workforce Manager and Developer: Technical Competencies and Proficiency Levels |
|---------------------------------------------|---------------------------------|----------------|----------------|----------------|----------------|
|                                            | Technical Competency             | GS-5 | GS-7/9 | GS-11/12 | GS-13 | GS-14/15 |
| Workforce Management                        |                                 | 1    | 1      | 3        | 3     | 4         |
| Project Management                           |                                 | 0    | 1      | 2        | 3     | 3         |
| Legal Advice and Advocacy                   |                                 | 0    | 1      | 2        | 3     | 4         |
| Risk Management                              |                                 | 0    | 0      | 2        | 3     | 4         |
| Strategic Planning                           |                                 | 1    | 1      | 2        | 3     | 4         |
| Policy Management                            |                                 | 1    | 1      | 2        | 3     | 4         |
| Training, Education and Awareness           |                                 | 1    | 1      | 3        | 3     | 2         |
I have one question left for you

Will you be a part of the solution?

To close the cybersecurity skill gap, we need everyone working towards the same goals. Here’s how you can help:

- Train the basics
- Use the NICE Cybersecurity Workforce Framework
- Work with partners across the education pipeline to increase knowledge and interest in cybersecurity
- Spread the word
Contacts

CISACareers@hq.dhs.gov
CISASTudentCareers@hq.dhs.gov
www.cisa.gov

@CISAgov
@Cyber

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
For more information:
cisa.gov
niccs.us-cert.gov

Questions?
Email: Zia.Anderson@dhs.gov