CYBERSECURITY WORKFORCE DEVELOPMENT TOOLKIT

How to Build a Strong Cybersecurity Workforce

U.S. DEPARTMENT OF HOMELAND SECURITY

Updated November 2016

WHAT IS CYBERSECURITY?

Cybersecurity refers to the technologies and techniques used to protect information and systems from being stolen, compromised or attacked. This includes unauthorized or criminal use of electronic data, attacks on networks and computers, and viruses and malicious codes. Cybersecurity is a national priority and critical to the well-being of all organizations. Start building your cybersecurity workforce today. Together, we can build a skilled and cyber-capable workforce to meet the cybersecurity challenges of the future.

ABOUT PLANNING YOUR CYBERSECURITY WORKFORCE

Cybersecurity professionals have unique skills, are in short supply, and are vital to our nation's security. As a result, competition for talent is fierce and establishing a strong team is essential. This requires organizations to tailor how they plan for their cybersecurity workforce so they have the right people in the right positions. The Department of Homeland Security (DHS) is committed to strengthening the workforce to help ensure we have skilled cybersecurity workers today and a strong pipeline of future cybersecurity leaders.

This kit will help you strengthen your organization through tools to help you understand your organization's cybersecurity workforce risks and take inventory of your workforce, templates to create your own cybersecurity career paths, and resources to recruit and retain top cybersecurity talent. Before getting started, familiarize yourself with key cybersecurity workforce design concepts and best practices:

Cybersecurity Workforce Planning Diagnostic

Cybersecurity Capability Maturity Model

Best Practices for Planning a Cybersecurity Workforce

National Cybersecurity Workforce Framework

DHS CMSI PushButtonPD™ Tool

Cybersecurity Training Catalog

HOW TO USE THE TOOLKIT

This kit has the resources and information you need to plan, build, and advance your cybersecurity workforce. How you use this toolkit is up to you: use the kit to start conversations with managers about building their cybersecurity teams, talk with employees about professional development, and/or integrate the concepts found in this toolkit into strategic planning efforts for future staffing needs. This kit is meant for Leaders and Program/Function Managers in large government and private organizations, including Human Resources, Information Security, Risk Management, Information Technology and Cybersecurity. For more information email niccs@hq.dhs.gov.

WHAT'S INSIDE?

This kit has a number of tools to help you build your cybersecurity workforce. All of the content can be found online at https://niccs.us-cert.gov/. Adapt the content for your organization's specific cybersecurity needs.

PREPARE

Assess Your Organization's Cybersecurity Workforce Planning Readiness

I need to determine how ready my organization is to conduct cybersecurity workforce planning.

PLAN

How to Plan for your Cybersecurity Team

I need to determine my cybersecurity risk exposure and risk tolerance.
I need help inventorying my cybersecurity workforce.
I need to determine and address my cybersecurity workforce gaps.

BUILD

What Should a Cybersecurity Team Look Like?

I need a better understanding of the NICE Cybersecurity Workforce Framework.
I need to create a cybersecurity position description.
I need help identifying traits of high-performing cyber professionals.
I need guidance for how to recruit cyber talent.

ADVANCE

Develop Your People

I need help creating cybersecurity career paths.
I need tips for retaining cyber staff at every level.
I need suggestions for professional development opportunities for my cyber workforce.

ASSESS YOUR ORGANIZATION'S CYBERSECURITY WORKFORCE PLANNING READINESS

A first step in preparing to build your cybersecurity workforce is having a shared vision for organizing your cybersecurity workforce against cybersecurity work. Having a common understanding supports leaders in responding to changing environments – giving you data to better adjust resources, see patterns of work, and highlight areas of potential risk. This is especially important in the ever-changing environment of cybersecurity.

To understand your organization's readiness to begin assessing your cybersecurity workforce, explore the **Cybersecurity Workforce Planning Capability Maturity Model (CMM).** The CMM is a self-evaluation tool to help organizations evaluate the maturity of their cybersecurity workforce planning capability.

DOWNLOAD

How Mature is Your Cybersecurity Workforce Planning Capability?

Each organization is unique. Some may not need their workforce planning capability to reach the *Optimizing* state. The CMM helps you identify with one of these levels and determine where to best apply your organization's planning resources:

Workforce Planning Maturity Levels

○	◐	●
LIMITED	**PROGRESSING**	**OPTIMIZING**
The most basic level, with a cybersecurity workforce planning capability in its infancy. For example, this organization may have limited established processes, lack of clear planning guidance, and limited data and analysis methods.	This level indicates some aspects of cybersecurity workforce planning throughout the organization that have started to perform and establish some infrastructure to support planning efforts.	The highest level of maturity, indicates workforce planning capabilities that are fully developed, are integrated with other business processes, and can support different levels of workforce and workload analysis.

PLAN

HOW TO PLAN FOR YOUR CYBERSECURITY TEAM

Your organization must ensure protection against threats to information systems. Unchecked risk puts any organization in jeopardy. Security breaches are often caused not by breakdown in technology, but by breakdown in organizational structure or workforce. To plan for protection, you need a good understanding of your current cybersecurity workforce as well as a strategy for the structure and management of that workforce for the future.

Below are the first five (5) steps to start planning for your cybersecurity team, including developing an inventory of your current cybersecurity workforce, understanding workload and staffing levels, and beginning to address any gaps.

1. **Explore Your Cybersecurity Risks:** Gain foundational knowledge about your cybersecurity workforce risk and the extent to which your organization can tolerate the potential outcomes. Increased risk places greater demands on your workforce and drives much of your future cybersecurity workforce needs.

   To help identify your general cybersecurity risk exposure and risk tolerance, and tailor your cybersecurity workforce planning to better predict future need, use the **Cybersecurity Workforce Planning Diagnostic**. Separate sections for government and private organizations are included. While the Diagnostic will help identify general cybersecurity risk exposure and risk tolerance (i.e. your risk profile), it is not a substitute for in-depth, organization-specific risk assessment and analysis in collaboration with leadership, human capital experts and cybersecurity managers.

   DOWNLOAD

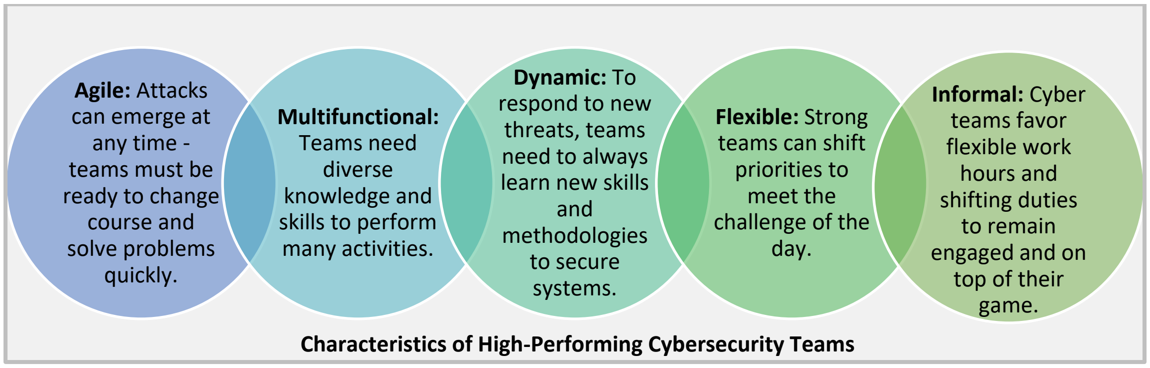
2. **Inventory Your Cybersecurity Workforce:** Work with your cybersecurity managers to quantify the size of your cybersecurity team, number of vacancies, identify the team's skills, and capture the activities they perform.

   → **Government organizations** – Access the Office of Personnel Management's (OPM) Information Technology Workforce Assessment for Cybersecurity (ITWAC) Summary Report to see a count of staff performing cybersecurity work, as well as training needs and workforce demographics (e.g., proficiency levels, background).

   → **Private organizations** – A tool to help inventory your cybersecurity workforce is forthcoming. This toolkit will be updated to provide this tool.

Use the results as a baseline to understand the current state of your organization's cybersecurity workforce. Refresh your workforce analysis on an annual basis.

As you take inventory of your cybersecurity staff skills, also consider the following recommended characteristics of high-performing cybersecurity teams. Use these characteristics as an additional guide to determine current and future staffing needs.



Agile: Attacks can emerge at any time - teams must be ready to change course and solve problems quickly.

Multifunctional: Teams need diverse knowledge and skills to perform many activities.

Dynamic: To respond to new threats, teams need to always learn new skills and methodologies to secure systems.

Flexible: Strong teams can shift priorities to meet the challenge of the day.

Informal: Cyber teams favor flexible work hours and shifting duties to remain engaged and on top of their game.

Characteristics of High-Performing Cybersecurity Teams

3. **Determine Any Gaps:** Evaluate your organization's risk profile and workforce planning recommendations from step 1 (Workforce Planning Diagnostic) against your workforce inventory in step 2 to begin to determine future needs and close gaps. For example:
   - ✓ List the skills needed to meet your team's workload and the types/number of professionals you need to develop internally or recruit externally
   - ✓ Determine hiring targets for vacancies and initiate recruiting (see *Build* section for cybersecurity-specific tips)

4. **Address the Gaps:** Below are examples of steps you can take to address the gaps identified in your organization's cybersecurity workforce inventory.
   - ✓ Consider adjusting the mix of positions and skills that make up your cybersecurity workforce
   - ✓ Search the **NICCS Training Catalog** to identify training for your workforce:

     GO
   - ✓ Determine if you can assign additional job duties to existing staff
   - ✓ Develop a program to create future cybersecurity leaders
   - ✓ Convene an internal panel of decision makers. Consider including:
     - o Senior leaders
     - o Financial and budgetary representatives
     - o Human capital experts
     - o Cybersecurity managers
   - ✓ Consider aligning the workforce planning process to your organization's budgetary process to ensure funding for cybersecurity positions

5. **Review and Update:** Once you have completed the first four steps, revisit the CMM in the *Prepare* section to determine additional ways to further your planning capability.

WHAT SHOULD A CYBERSECURITY TEAM LOOK LIKE?

One way to ensure you have the right cybersecurity team is to align to current national standards. The NICE Cybersecurity Workforce Framework (Workforce Framework) is the standard for defining your cybersecurity workforce. Align position descriptions, job duties, and skill requirements to the Workforce Framework to operate successfully. For example, you can use Specialty Area definitions, as well as Tasks and Knowledge, Skills and Abilities (KSAs), to develop position descriptions and establish competency models.

What is the NICE Cybersecurity Workforce Framework?

The Workforce Framework is the foundation for all cyber workforce development activities and was created to increase the size and capability of the U.S. cybersecurity workforce.

- Organizes cybersecurity work into 7 Categories and 33 Specialty Areas
- Identifies the Tasks and Knowledge, Skills, and Abilities (KSAs) required to complete cyber work

An updated version of the Workforce Framework will be released in 2017 as Special Publication 800-181 by the National Institute of Standards and Technology (NIST). It will include a new layer of specificity – Work Roles – which will provide lists of KSAs that roles must have in order to perform a specific set of Tasks. 50+ Work Roles will be organized under Specialty Areas. With this addition, organizations will more easily be able to align positions to the Workforce Framework.

1. **Explore the Workforce Framework.**

   GO

2. **Align your Cybersecurity Workforce to National Standards:** Understand how each position aligns to the Workforce Framework to uncover potential skill gaps.
   - **Choose from the Work Roles** (found in the Workforce Framework) for each position that performs cybersecurity work
   - **Compare current tasks performed to additional tasks recommended** for each Specialty Area

3. **Use the DHS CMSI PushButtonPD™ Tool to create custom cyber-specific positions for your organization.**

   Federal organizations can use the **DHS CMSI PushButtonPD™ Tool** to quickly draft a federal employee Position Description (PD) without extensive training or prior knowledge of position classification. This tool creates a robust hiring package that can easily be integrated into existing agency HR processes.

GO

Non-Federal organizations can use the following template to populate the highlighted fields with information that meets the needs of your organization (you can find Specialty Areas and Task examples in the Workforce Framework).

Position Title	*[Fill in Position Title]*
Primary Specialty Area(s)	*[Fill in Specialty Area(s)]*
Secondary Specialty Area(s)	*[Fill in Specialty Area(s)]*
Current Tasks Performed (i.e., specific job duties)	
Additional Tasks recommended by Specialty Area	

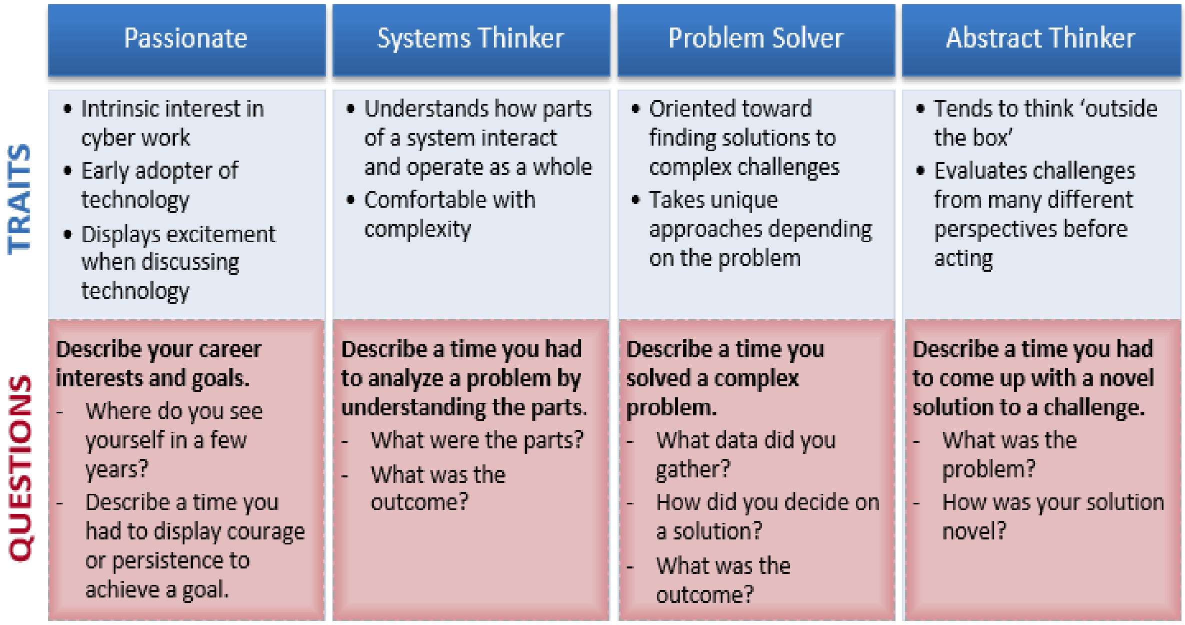
What to Look for in High-Performing Cybersecurity Professionals

Another important part of building a cybersecurity team is knowing the unique characteristics you want to add to your team. Whether your organization is looking to hire one cybersecurity professional or build a whole team, understanding what makes a cybersecurity professional tick is important to attracting - and keeping - the right team. The table below features many of the traits of top cybersecurity professionals. (Also refer to the list on page five of this kit for high-performing *team* characteristics).

Review this table and consider if individuals on your team with skills from the Workforce Framework also have these traits; how might they expand their skills to fill your need?

Also, think about how you might change your approach to attracting cybersecurity professionals to better identify individuals with these attributes.

For example, **use these questions to interview candidates for your cybersecurity team.**



	Passionate	Systems Thinker	Problem Solver	Abstract Thinker
TRAITS	• Intrinsic interest in cyber work • Early adopter of technology • Displays excitement when discussing technology	• Understands how parts of a system interact and operate as a whole • Comfortable with complexity	• Oriented toward finding solutions to complex challenges • Takes unique approaches depending on the problem	• Tends to think 'outside the box' • Evaluates challenges from many different perspectives before acting
QUESTIONS	**Describe your career interests and goals.** - Where do you see yourself in a few years? - Describe a time you had to display courage or persistence to achieve a goal.	**Describe a time you had to analyze a problem by understanding the parts.** - What were the parts? - What was the outcome?	**Describe a time you solved a complex problem.** - What data did you gather? - How did you decide on a solution? - What was the outcome?	**Describe a time you had to come up with a novel solution to a challenge.** - What was the problem? - How was your solution novel?

How to Recruit Top Cybersecurity Talent

Use the Cybersecurity Recruitment Activity Checklist to build a cybersecurity workforce that meets the needs of your organization.

Cybersecurity Recruitment Activity Checklist

Use the checklist to recruit top cybersecurity talent.

IDENTIFY VACANT POSITION(S)

- ❑ Work with hiring managers and workforce planners to determine cybersecurity recruiting needs
- ❑ Identify cybersecurity-specific hiring flexibilities (e.g., hiring bonuses)
- ❑ Use the workforce planning tools and cybersecurity traits profiles included in this toolkit to identify target population characteristics, work preferences, technical background, and current cybersecurity trends to increase job interest

EVALUATE POTENTIAL SOURCES FOR THE TALENT PIPELINE

- ❑ Create a comprehensive list of current and potential recruiting alliances that align with organizational goals and resources (e.g., Centers of Academic Excellence (CAEs)), colleges, universities, cybersecurity competitions, and Veterans transition programs)
- ❑ Prioritize where and how to recruit cybersecurity professionals (e.g. online job search engines, hackathons, cyber competitions, personal referrals, social media)
- ❑ Identify current cybersecurity employees who can engage with potential candidates at recruiting events (e.g., job fairs, campus recruiting events)

- □ Establish an employee referral program to recruit talented and trusted cybersecurity professionals from your cybersecurity employees' personal networks (e.g., colleges/universities, alma maters, professional associations)

DEVELOP MARKETING STRATEGY & MATERIALS

- □ Develop a list of advantages and benefits of the position(s) and your organization (i.e., selling points) to incorporate into outreach efforts and materials. Think about the trait profiles on the previous page to appeal to the best talent
- □ Highlight key technology, tools, and IT capabilities to attract the right cybersecurity talent for your organization's specific risk profile from page four of this kit
- □ Develop materials (e.g., slick sheets, job announcements, social media messages)
- □ Consider using interactive communication tools, such as social media (e.g., Twitter), that live where cybersecurity professionals do – the internet – to recruit
- □ Schedule and announce interaction opportunities (e.g. webinars, live Tweeting)

SELECT AND HIRE

- □ Use the cybersecurity trait profiles and interview questions provided in this toolkit to evaluate non-technical characteristics of cybersecurity professionals
- □ If a decision to hire candidate is made, create a competitive offer package to attract top cybersecurity talent, considering the development items in the next section

ADVANCE

Develop Your People

Retain Staff at Every Level

Whether entry level, mid-career or seasoned cybersecurity professionals, here are some simple steps you can take to recognize, develop and retain staff at every level. Use the profiles below as a guide to understand which of the steps outlined in the Advance section will best support the specific type of cybersecurity professional your organization is looking to recruit and retain.

Entry-Level Cyber Professional	Mid-Career Cyber Professional	Seasoned or Executive Cyber Professional
• College, graduate, post-graduate, and career changers new to cybersecurity. • Focused on learning cyber technical skillset and job requisites, acclimating to organizational environment, establishing support network, and gaining work experience.	• Professionals with previous cyber related experience and skills. • Focused on shaping career path and advancing technical skillset through job rotations, certifications, developing technology, and supervisory opportunities.	• Demonstrated cyber expertise and progressive leadership experience. • Focused on expanding technical expertise, making contributions to technical domain and broader cyber security community, and leadership development.
Tips to Retain Entry-Level Staff ❖ Foster an environment where diverse perspectives are welcome ❖ Encourage two-way dialogue for open communication ❖ Provide frequent feedback on job performance ❖ Ensure that cyber professionals have quality supervision and mentorship ❖ Provide opportunities to acquire new skills through established training, challenging job assignments, and career pathing ❖ Recognize staff for strong work performance	**Tips to Retain Mid-Career Staff** ❖ Emphasize work-life balance; encourage taking time to pursue activities and interests ❖ Provide opportunities to obtain advanced training and certifications ❖ Allow information sharing within the organization and professional forums ❖ Offer challenging job assignments ❖ Include employees in decision making and innovation ❖ Implement reward programs	**Tips to Retain Executive Staff** ❖ Provide advanced training and development opportunities ❖ Create tailored development plans that identify leadership competencies and areas for development ❖ Recognize leaders for their successes and accomplishments ❖ Consider performance and loyalty-based bonuses to retain staff ❖ Promote cyber executives to develop intellectual capital and create information sharing mechanisms

Help Your Staff Navigate Cybersecurity Careers

Once you have the cybersecurity team you need inside your organization, it is equally important to take measures to grow and keep that staff. According to the September 2016 State of Cyber Security Professional Careers, approximately 46% of respondents (cybersecurity professionals) reported that they were solicited for jobs at other companies at least once per week. It's important that HR professionals and cybersecurity managers work together to retain cybersecurity professionals, and help staff develop career paths inside your organization. Develop and share career paths with employees to help staff identify their proficiency levels and advance in their chosen paths.

Here are three (3) steps you can take to start building your organization's cybersecurity career path.

Step 1 – Familiarize yourself with proficiency levels and review sample career paths.

Sample Proficiency Levels

BEGINNER	INTERMEDIATE	SENIOR/EXPERT
Ability to apply basic knowledge and skills in simple work situations with specific instructions and/or guidance	Ability to apply knowledge and skills in straightforward, routine work situations with limited need for direction	Ability to apply advanced knowledge and skills in complex, difficult, or novel work situations; is an acknowledged authority, advisor, or key resource in a given topic

Sample Career Paths

CAREER PATH: BEGINNER LEVEL		
Suggested Experience & Credentials	**Sample KSAs / Skills**	**Suggested Training & Development Activities**
Bachelor's Degree from an accredited program in a Computer Science-related field OR 2 years relevant work experience	Sample KSAs • Vulnerabilities Assessment o Skill in the use of penetration testing tools and techniques • Information Security/Assurance o Skill in performing damage assessments Sample Non-Technical Skills • Critical Thinking & Analytical Skills • Written & Oral Communication	Sample Development Activities • University Programs (e.g., George Mason University; Stevens Institute of Technology; Carnegie Mellon University) • Government agency courses (e.g., IRM-NDU, NSA, DoD, Department of State DSTC, DHS certifications)

ADVANCE

CAREER PATH: INTERMEDIATE LEVEL

Suggested Experience & Credentials	Sample KSAs / Skills	Suggested Training & Development Activities
Bachelor's Degree from an accredited program in a Computer Science-related field plus 3 years of relevant work experience; OR 6 years relevant work experience Possession and demonstrated application of relevant certifications (as determined by the department/agency): Information systems security certifications (e.g., (ISC)² CSSLP and CISSP, various SANS certifications, EnCase Cybersecurity suite, GIAC Security Essentials Certification (GSEC), and relevant programming languages)	Sample KSAs • Vulnerabilities Assessment o Ability to identify systemic security issues based on the analysis of vulnerability and configuration data o Skill in the use of penetration testing tools and techniques • Information Security/Assurance o Skill in performing damage assessments • Computer Network Defense o Skill in detecting host and network-based intrusions Sample Non-Technical Skills • Critical Thinking & Analytical Skills • Written & Oral Communication	*No UMUC or SANS courses considered map to this specialty area at the Full Performance level Sample Development Activities • University Programs (e.g., George Mason University; Stevens Institute of Technology; Carnegie Mellon University) • Formal training programs/seminars (e.g., GIAC-Auditing Networks, Perimeters & Systems) • Government agency courses (e.g., IRM-NDU, NSA, DoD, Department of State DSTC, DHS certifications) • Joint Duty Assignments

ADVANCE

CAREER PATH: SENIOR/EXPERT LEVEL

Suggested Experience & Credentials	Sample KSAs / Skills	Suggested Training & Development Activities
Master's Degree from an accredited program in a Computer Science-related field plus 5 years of relevant work experience; OR Bachelor's degree plus 10 years relevant work experience and project management experience Possession and demonstrated application of relevant certifications (as determined by the department/agency): PMP, Information systems security certifications (e.g., (ISC)^2 CSSLP and CISSP, various SANS certs, EnCase Cybersecurity suite, GIAC Security Essentials Certification (GSEC), ISACA Certified Information Security Manager Certification (CISM), Security Certified Network Professional (SCNP), IT/Business Systems Audit certifications (e.g., CISA, GSNA), and relevant programming languages)	Sample KSAs • Vulnerabilities Assessment o Ability to identify systemic security issues based on the analysis of vulnerability and configuration data o Knowledge of application vulnerabilities o Skill in the use of penetration testing tools and techniques • Information Security/Assurance o Skill in performing damage assessments • Computer Network Defense o Skill in mimicking threat behaviors o Skill in detecting host and network-based intrusions via intrusion detection technologies (e.g., Snort) Sample Non-Technical Skills • Critical Thinking & Analytical Skills • Attention to Detail • Creative Problem Solving • Written & Oral Communication • Project/Program Management • Leadership & People Management • Influencing/Negotiating	Training – UMUC • INFA660 Security Policy, Ethics and the Legal Environment Sample Development Activities • University Programs (e.g., George Mason University; Stevens Institute of Technology; Carnegie Mellon University) • Formal training programs/seminars (e.g., GIAC-Auditing Networks, Perimeters & Systems) • Participation in community organizations and working groups (e.g., Federal Information Systems Security Educators Association (FISSEA), Information Systems Security Association (ISSA)) • Joint Duty Assignments • Participation in professional associations, communities, practice or network groups in the field to share best practices, trends • Developing white papers and policies • Participating in professional coaching sessions, particularly for general competencies • Participation in security and cyber relevant conferences (i.e. BlackHat, Defcon, Shmoocon, RSA, CANSEC West, others)

ADVANCE

Step 2 – Use the following template to create custom cybersecurity-specific career paths for your organization. Populate the **highlighted** fields with information that meets the needs of your organization (KSAs can be found in the Workforce Framework)

CAREER PATH: *[LEVEL]*		
Suggested Experience & Credentials	Suggested KSAs / Skills *	Suggested Training & Development Activities
[DEGREE] from *[PROGRAM TYPE]* (plus) *[YEARS]* relevant work experience; OR *[YEARS]* relevant work experience Possession and demonstrated application of relevant certifications (as determined by the department/agency): [*CERTIFICATIONS]* and/or relevant programming languages	KSAs • *[KSA]* • *[KSA]* • *[KSA]* • *[KSA]* • *[KSA]* • *[KSA]* Non-Technical Skills • *[Varied based on level; e.g., communications, ability to listen and ask meaningful questions, skill in managing staff, skill in mentoring, strategic thinking]*	Training • *[COURSE]* Sample Development Activities • *[UNIVERSITY PROGRAMS]* • *[FORMAL TRAINING PROGRAMS/SEMINARS]* • *[GOVERNMENT AGENCY COURSES]* • *[ACTIVITY]* • *[ACTIVITY]*

* KSAs are found in the Workforce Framework; Non-technical skills are not cyber-specific – each organization will need to decide which non-technical skills are valued in their workforce. Existing organizational competency models commonly list non-technical skills.

Step 3 – Share career paths with cybersecurity managers and staff. Communications channels might include:

- Internal websites
- Employee communications
- Annual reviews

Professional Growth Opportunities for Your Cybersecurity Staff

In addition to career paths, your organization can provide a variety of professional growth opportunities to attract, engage, and retain cybersecurity professionals. Offering staff opportunities to think outside-the-box, solve complex cybersecurity challenges, and learn new cybersecurity skills may increase job satisfaction and improve retention. These opportunities also enable your staff to develop their skills for the quickly-evolving field of cybersecurity.

ADVANCE

SUPPLY AND DEMAND

- Visit cyberseek.org to learn more about the supply and demand of cybersecurity workers in your community
- Uncover additional market dynamics like in-demand skills and credentials, average salaries, and number of job openings
- Encourage staff to explore common cybersecurity roles and transition opportunities

TRAINING

- Direct all cybersecurity staff to more than 3,000 cyber training courses on the National Initiative for Cybersecurity Careers and Studies (NICCS) Training Catalog
- Government cybersecurity staff and veterans also have access to free courses through the Federal Virtual Training Environment (FedVTE) - Post the following FedVTE Flyer in your workplace
- Federal employees can also receive free, instructor-led, virtual training through FedVTE Live!

CERTIFICATIONS

- Earning certifications enables staff to stay current on in-demand skills and become leaders in the cybersecurity field
- Example Certifications:
    - CompTIA SECURITY+
    - Certified Information Systems Security Professional
    - GIAC Security Essentials (GSEC)

SHADOWING

- Staff gain on-the-job experience for a desired position
- Encourage staff to connect with cybersecurity colleagues; shadowing is a great way to network and learn from others

MENTORING

- Encourage cybersecurity staff to establish mentoring relationships to learn from seasoned cybersecurity professionals

CONFERENCES & PROFESSIONAL ORGANIZATIONS

- Employees can stay up-to-date with developments in the field and network with fellow cybersecurity professionals
- Example Conferences:
    - NICE Conference & Expo
    - RSA Security Conference
    - NSA Information Assurance Symposium
- Example Professional Organization:
    - Information Systems Security Association

CYBERSECURITY AWARENESS

Stop.Think.Connect.™

- National public awareness campaign aimed at increasing the understanding of cybersecurity threats and empowering all Americans to be safer and more secure online. Resources are available at www.dhs.gov/stopthinkconnect
- October is National Cyber Security Awareness Month. Learn more at www.dhs.gov/national-cyber-security-awareness-month

TOP CYBERSECURITY SCHOOLS

- Centers of Academic Excellence (CAE) in Cyber Defense: DHS/NSA designated over 230 institutions where employees can pursue degrees
- For more information visit the CAE Site or email askCAEIAE@nsa.gov
- The Scholarship for Service (SFS) provides funding to full-time students in exchange for government service. Learn more here

TELL US WHAT YOU THINK

The field of cybersecurity is ever-changing. If you have ideas on additional resources that will help you plan for, build, and advance your cybersecurity workforce, please email us at niccs@hq.dhs.gov.