Homeland Security

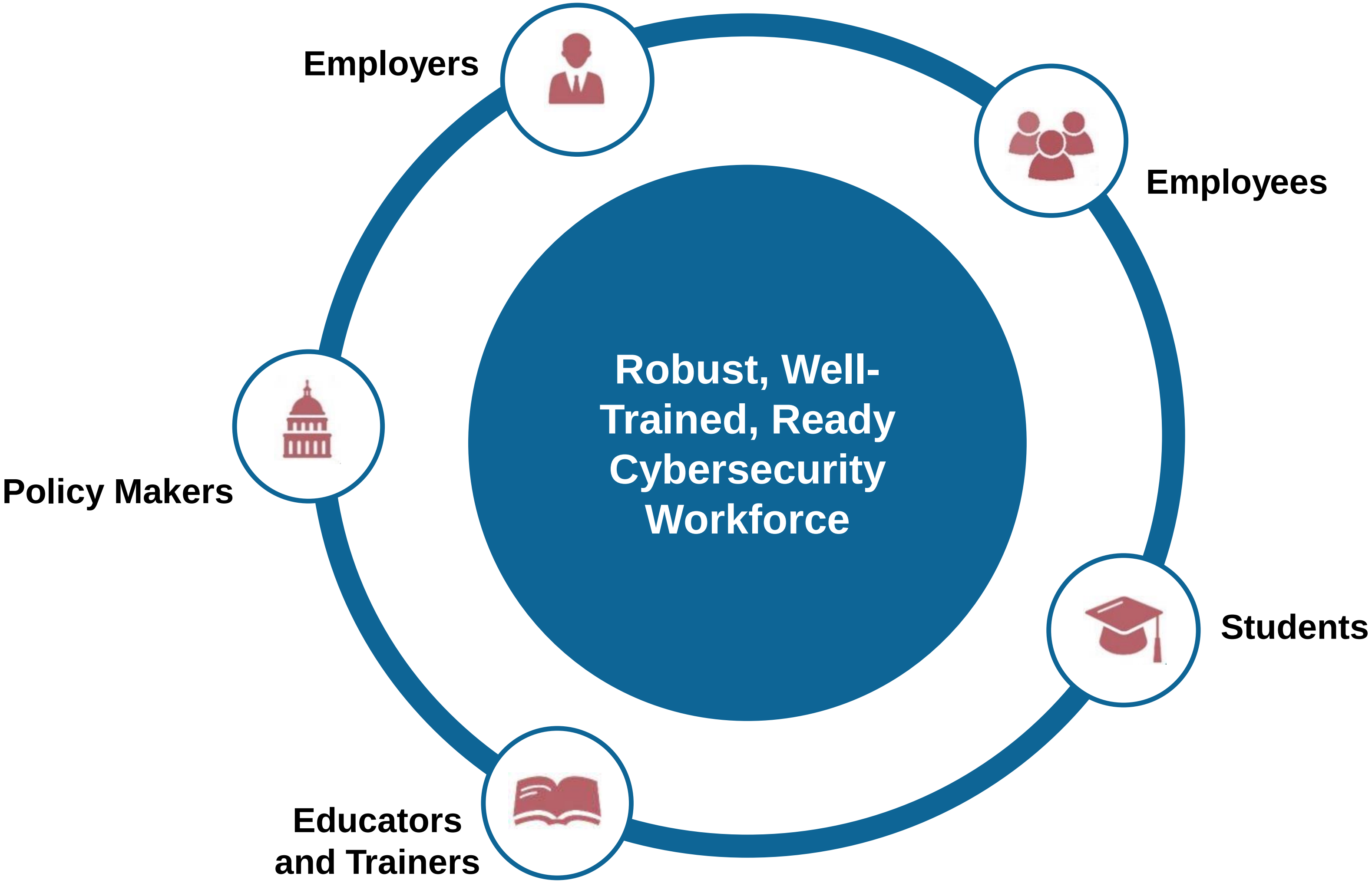
Build Your Cybersecurity Team: Create a Strong Cybersecurity Workforce Using Best Practices in Development

Noel Kyle, Program Manager
Department of Homeland Security (DHS)
National Cybersecurity Education & Awareness Branch (CE&A)

November 2017

The Cybersecurity Workforce Challenge

Vision for the Nation’s Cybersecurity Workforce



Employers

Employees

Policy Makers

Robust, Well-Trained, Ready Cybersecurity Workforce

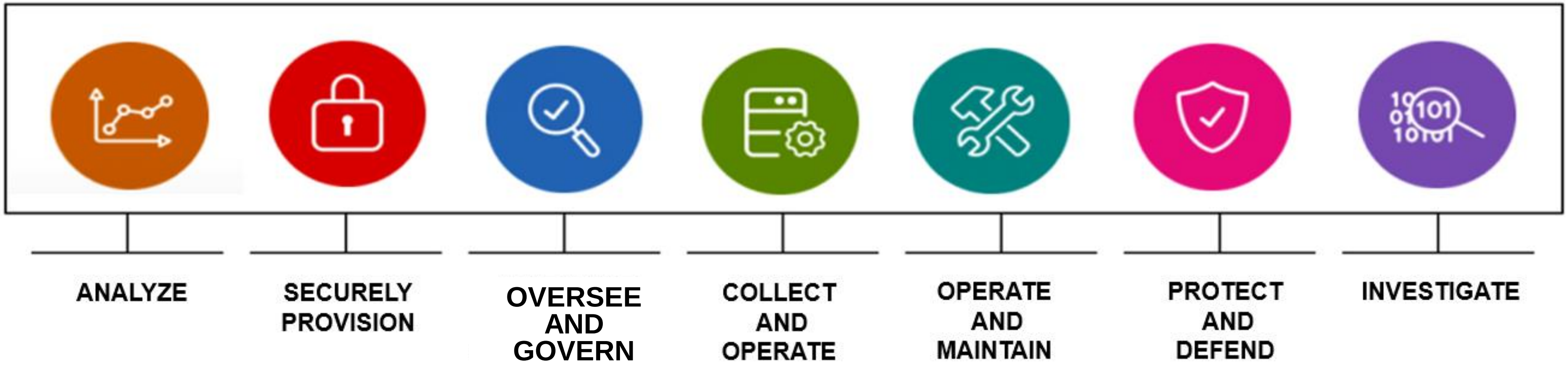
Students

Educators and Trainers

Foundation for the Cybersecurity Workforce

NICE Cybersecurity Workforce Framework

- Describes cybersecurity work
- 7 Categories, 30+ Specialty Areas, 50+ Work Roles
- Current version in NIST SP 800-181 is 3rd iteration
- Competencies are planned to be added in 2018



Historical Codes Mapped to New Work Role Codes

ANALYZE – 10

Warning Analyst – 141
Exploitation Analyst – 121
All-Source Analyst – 111
Mission Assessment Specialist – 112
Target Developer – 131
Target Network Analyst – 132
Multi-Disciplined Language Analyst – 151

COLLECT & OPERATE – 30

All Source-Collection Manager – 311
All Source-Collection Requirements Manager – 312
Cyber Intel Planner – 331
Cyber Ops Planner – 332
Partner Integration Planner – 333
Cyber Operator – 321

OPERATE & MAINTAIN – 40

Database Administrator – 421
Data Analyst – 422
Knowledge Manager – 431
Technical Support Specialist – 411
Network Operations Specialist – 441
System Administrator – 451
Systems Security Analyst – 461

INVESTIGATE – 20

Cyber Crime Investigator – 221
Forensics Analyst – 211
Cyber Defense Forensics Analyst – 212

PROTECT & DEFEND – 50

Cyber Defense Analyst – 511
Cyber Defense Infrastructure Support Specialist - 521
Cyber Defense Incident Responder – 531
Vulnerability Assessment Analyst – 541

SECURELY PROVISION – 60

Authorizing Official/Designating Representative – 611
Security Control Assessor – 612
Software Developer – 621
Secure Software Assessor – 622
Enterprise Architect – 651
Security Architect – 652
Research & Development Specialist – 661
Systems Requirements Planner – 641
System Testing and Evaluation Specialist – 671
Information Systems Security Developer – 631
Systems Developer – 632

OVERSEE & GOVERN – 70

Cyber Legal Advisor – 731
Privacy Compliance Manager – 732
Cyber Instructional Curriculum Developer – 711
Cyber Instructor – 712
Information Systems Security Manager – 722
COMSEC Manager – 723
Cyber Workforce Developer and Manager – 751
Cyber Policy and Strategy Planner – 752

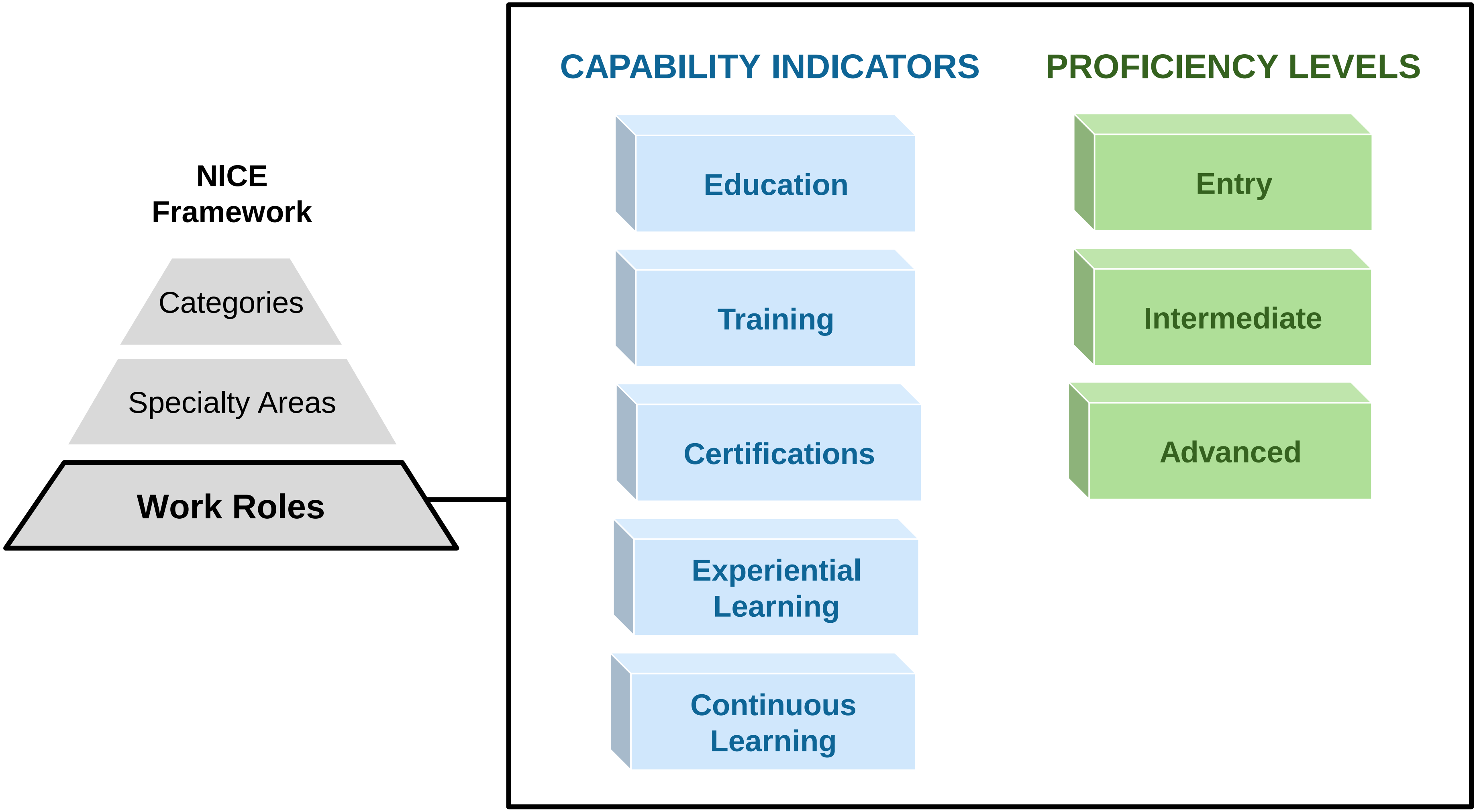
CYBERSECURITY PROGRAM / PROJECT MANAGEMENT – 80

Program Manager – 801
IT Project Manager – 802
Product Support Manager – 803
IT Investment/Portfolio Manager – 804
IT Program Auditor – 805

EXECUTIVE CYBER LEADERSHIP – 90

Executive Cyber Leadership – 901

Work Role Capability Indicators



Capability Indicator Development

Background

- Introduction of Work Roles in NIST Special Publication 800-181
- DoD project to define qualification requirements
- Continued cybersecurity risk and the state of workforce development

Methodology

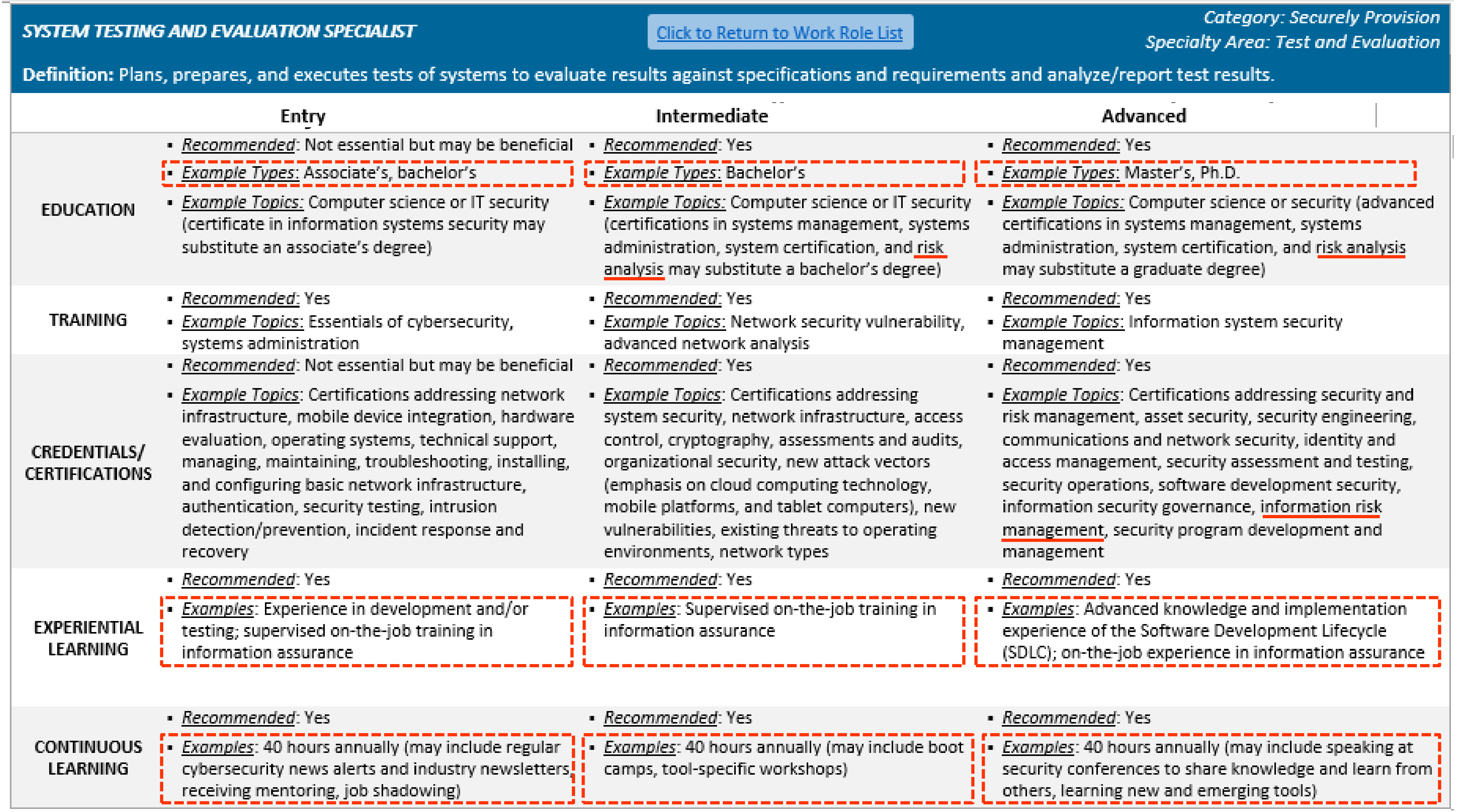
- Outreach – Invitations sent to 1,000+ potential participants
- Data Collection Sources –
  - Focus groups
  - Phone interviews
  - Table questionnaire distributed via email
  - Supplemental data from DHS, HHS, and Navy

Role	**Secure Software Assessor (Example)**		
Proficiency Level	*Entry*	*Intermediate*	*Advanced*
Capability Indicator	Education	Education	Education
	Training	Training	Training
	Credentials/ Certifications	Credentials/ Certifications	Credentials/ Certifications
	Experiential Learning	Experiential Learning	Experiential Learning
	Continuous Learning	Continuous Learning	Continuous Learning

Overall Findings

1. Higher education can be beneficial but is not always necessary for entry level
2. Certifications are often considered indicators of ability
3. On-the-job experience is essential for management roles and at higher proficiency levels
4. Risk is the most frequently recommended training topic
5. Continuous learning is recommended at all levels but expectations vary based on level

Cybersecurity Workforce Capabilities (Example 1)



SYSTEM TESTING AND EVALUATION SPECIALIST

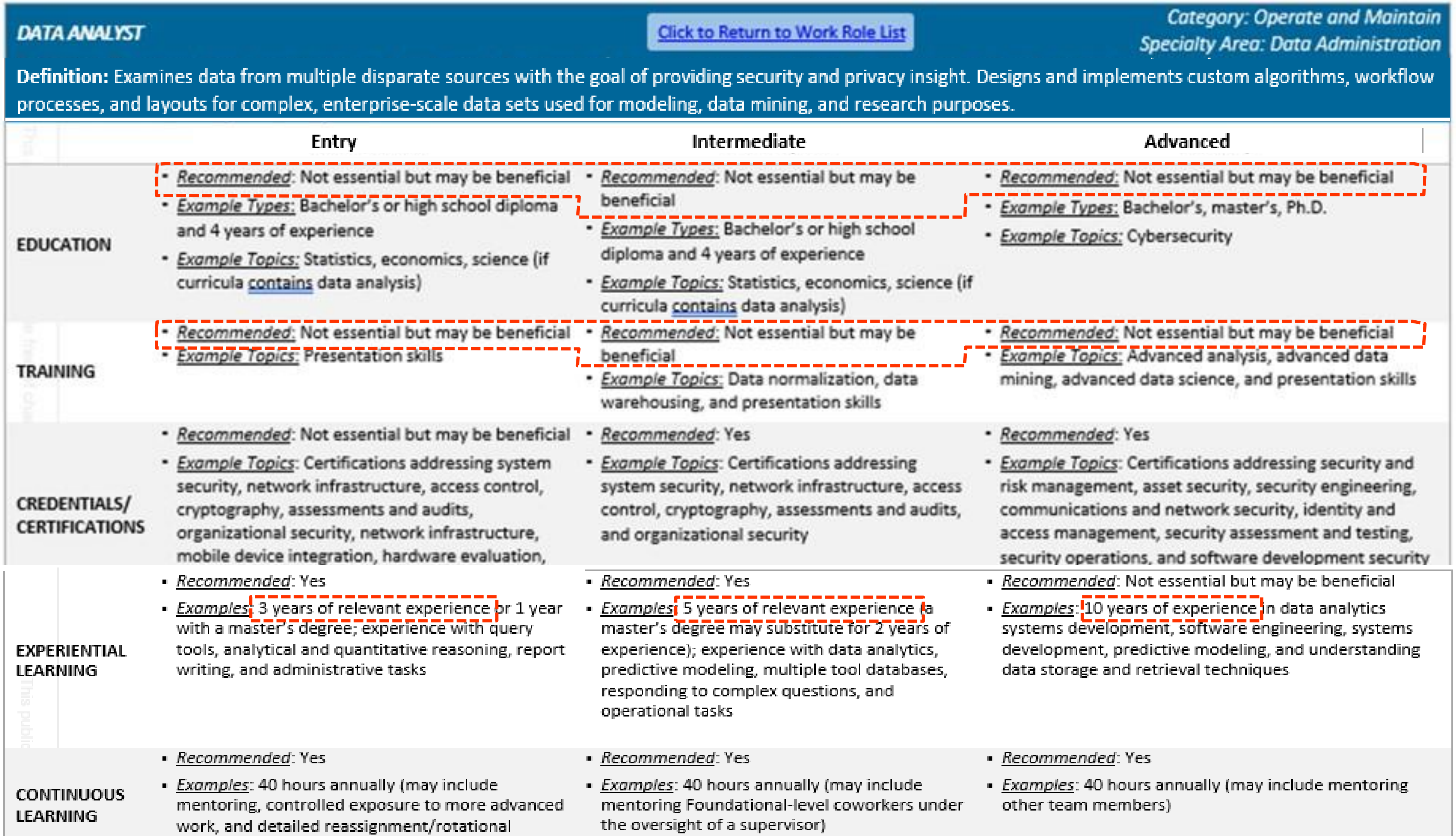
Click to Return to Work Role List

Category: Securely Provision
Specialty Area: Test and Evaluation

Definition: Plans, prepares, and executes tests of systems to evaluate results against specifications and requirements and analyze/report test results.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types:* Associate's, bachelor's ▪ *Example Topics:* Computer science or IT security (certificate in information systems security may substitute an associate's degree)	▪ *Recommended*: Yes ▪ *Example Types:* Bachelor's ▪ *Example Topics:* Computer science or IT security (certifications in systems management, systems administration, system certification, and risk analysis may substitute a bachelor's degree)	▪ *Recommended:* Yes ▪ *Example Types:* Master's, Ph.D. ▪ *Example Topics:* Computer science or security (advanced certifications in systems management, systems administration, system certification, and risk analysis may substitute a graduate degree)
TRAINING	▪ *Recommended:* Yes ▪ *Example Topics:* Essentials of cybersecurity, systems administration	▪ *Recommended*: Yes ▪ *Example Topics:* Network security vulnerability, advanced network analysis	▪ *Recommended:* Yes ▪ *Example Topics:* Information system security management
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, managing, maintaining, troubleshooting, installing, and configuring basic network infrastructure, authentication, security testing, intrusion detection/prevention, incident response and recovery	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, new attack vectors (emphasis on cloud computing technology, mobile platforms, and tablet computers), new vulnerabilities, existing threats to operating environments, network types	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, information security governance, information risk management, security program development and management
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: Experience in development and/or testing; supervised on-the-job training in information assurance	▪ *Recommended*: Yes ▪ *Examples*: Supervised on-the-job training in information assurance	▪ *Recommended*: Yes ▪ *Examples*: Advanced knowledge and implementation experience of the Software Development Lifecycle (SDLC); on-the-job experience in information assurance
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include regular cybersecurity news alerts and industry newsletters, receiving mentoring, job shadowing)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include boot camps, tool-specific workshops)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include speaking at security conferences to share knowledge and learn from others, learning new and emerging tools)

Cybersecurity Workforce Capabilities (Example 2)



DATA ANALYST

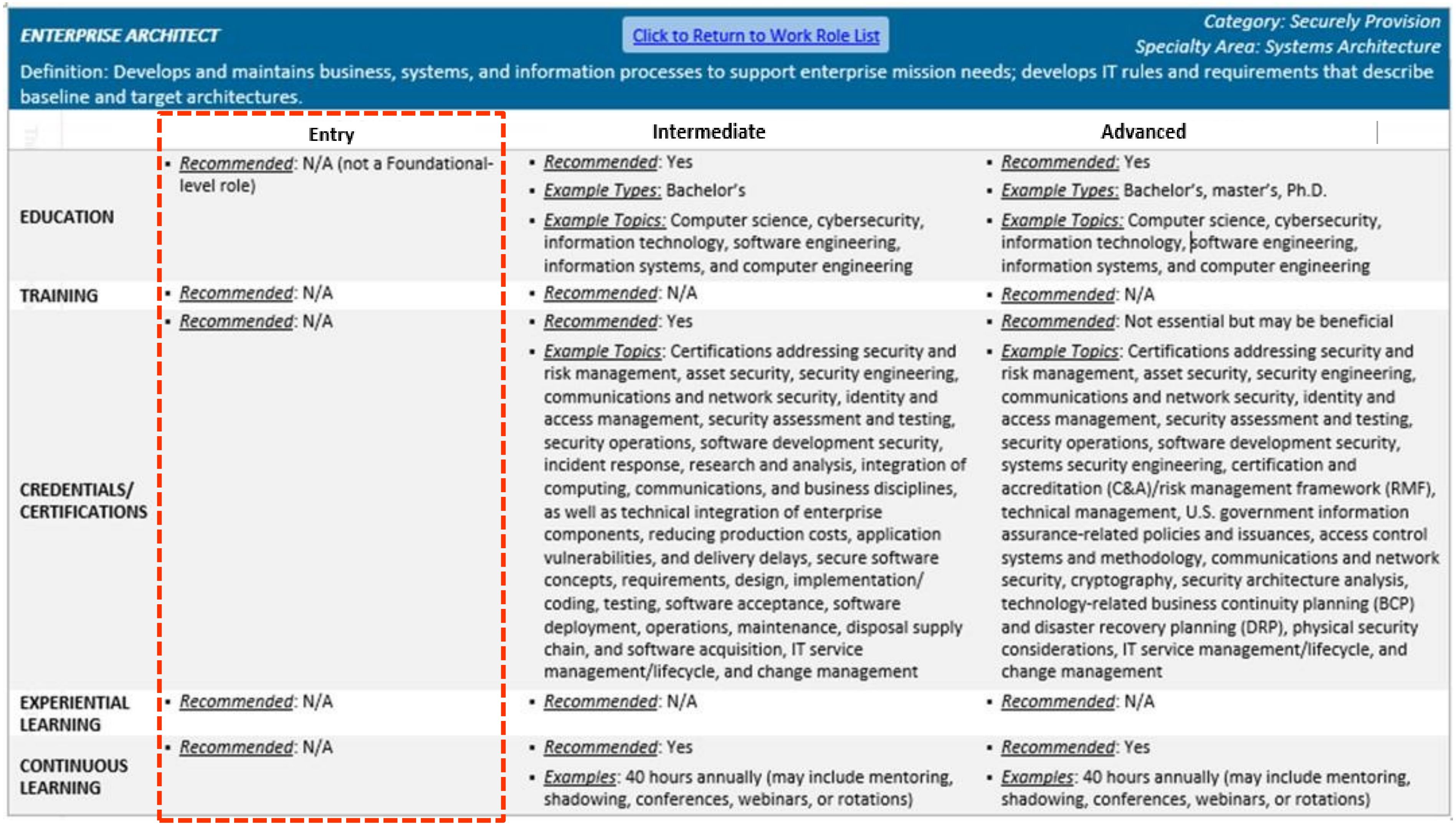
Click to Return to Work Role List

Category: Operate and Maintain
Specialty Area: Data Administration

Definition: Examines data from multiple disparate sources with the goal of providing security and privacy insight. Designs and implements custom algorithms, workflow processes, and layouts for complex, enterprise-scale data sets used for modeling, data mining, and research purposes.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types:* Bachelor's or high school diploma and 4 years of experience ▪ *Example Topics:* Statistics, economics, science (if curricula contains data analysis)	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types:* Bachelor's or high school diploma and 4 years of experience ▪ *Example Topics:* Statistics, economics, science (if curricula contains data analysis)	▪ *Recommended:* Not essential but may be beneficial ▪ *Example Types:* Bachelor's, master's, Ph.D. ▪ *Example Topics:* Cybersecurity
TRAINING	▪ *Recommended:* Not essential but may be beneficial ▪ *Example Topics:* Presentation skills	▪ *Recommended:* Not essential but may be beneficial ▪ *Example Topics:* Data normalization, data warehousing, and presentation skills	▪ *Recommended:* Not essential but may be beneficial ▪ *Example Topics:* Advanced analysis, advanced data mining, advanced data science, and presentation skills
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, network infrastructure, mobile device integration, hardware evaluation,	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, and organizational security	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security
EXPERIENTIAL LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 3 years of relevant experience or 1 year with a master's degree; experience with query tools, analytical and quantitative reasoning, report writing, and administrative tasks	▪ *Recommended*: Yes ▪ *Examples*: 5 years of relevant experience (a master's degree may substitute for 2 years of experience); experience with data analytics, predictive modeling, multiple tool databases, responding to complex questions, and operational tasks	▪ *Recommended*: Not essential but may be beneficial ▪ *Examples*: 10 years of experience in data analytics systems development, software engineering, systems development, predictive modeling, and understanding data storage and retrieval techniques
CONTINUOUS LEARNING	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, controlled exposure to more advanced work, and detailed reassignment/rotational	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring Foundational-level coworkers under the oversight of a supervisor)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring other team members)

Cybersecurity Workforce Capabilities (Example 3)



ENTERPRISE ARCHITECT

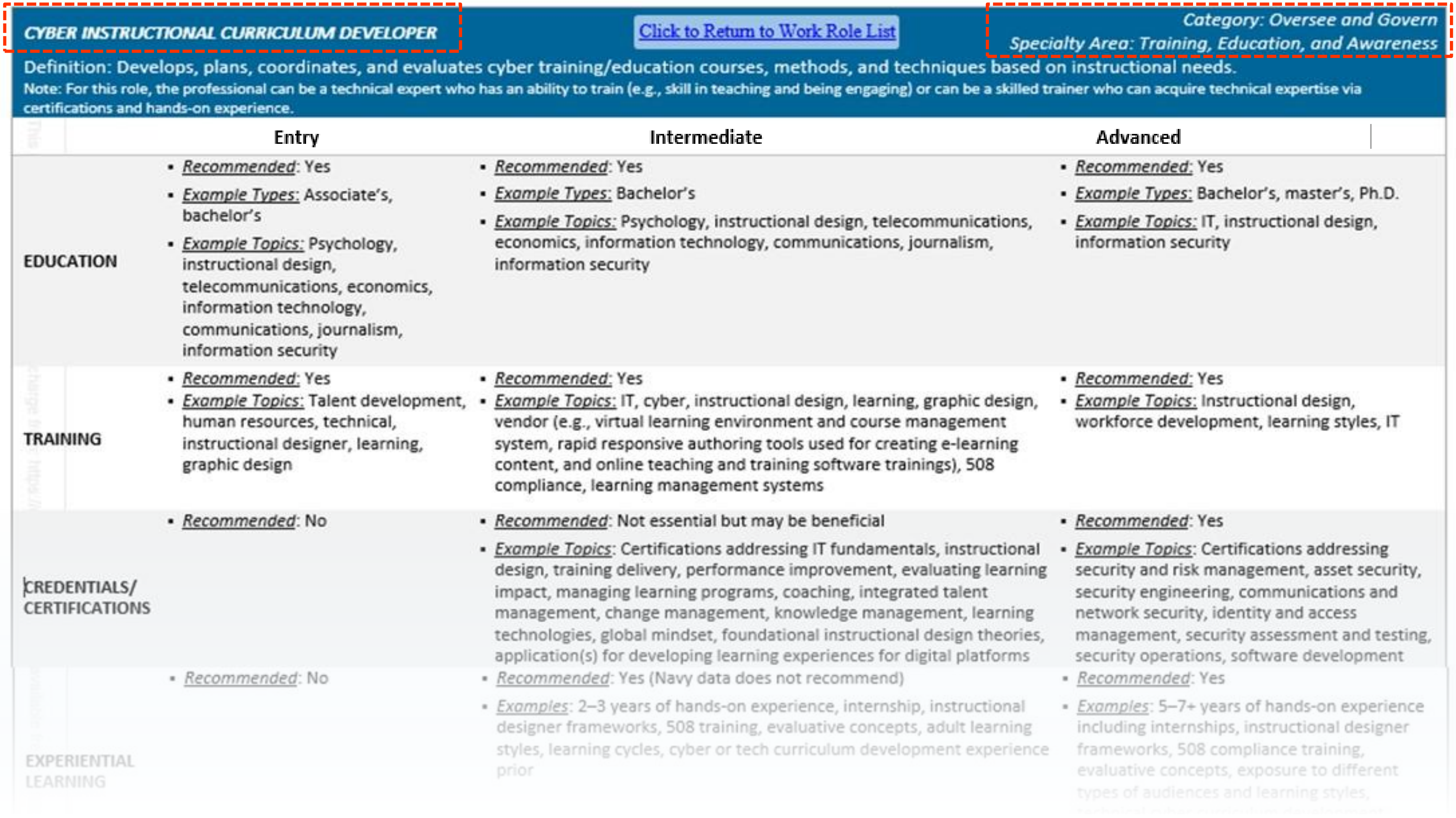
Click to Return to Work Role List

Category: Securely Provision
Specialty Area: Systems Architecture

Definition: Develops and maintains business, systems, and information processes to support enterprise mission needs; develops IT rules and requirements that describe baseline and target architectures.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: N/A (not a Foundational-level role)	▪ *Recommended*: Yes ▪ *Example Types:* Bachelor's ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering	▪ *Recommended*: Yes ▪ *Example Types:* Bachelor's, master's, Ph.D. ▪ *Example Topics:* Computer science, cybersecurity, information technology, software engineering, information systems, and computer engineering
TRAINING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, incident response, research and analysis, integration of computing, communications, and business disciplines, as well as technical integration of enterprise components, reducing production costs, application vulnerabilities, and delivery delays, secure software concepts, requirements, design, implementation/ coding, testing, software acceptance, software deployment, operations, maintenance, disposal supply chain, and software acquisition, IT service management/lifecycle, and change management	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, systems security engineering, certification and accreditation (C&A)/risk management framework (RMF), technical management, U.S. government information assurance-related policies and issuances, access control systems and methodology, communications and network security, cryptography, security architecture analysis, technology-related business continuity planning (BCP) and disaster recovery planning (DRP), physical security considerations, IT service management/lifecycle, and change management
EXPERIENTIAL LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: N/A	▪ *Recommended*: N/A
CONTINUOUS LEARNING	▪ *Recommended*: N/A	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)	▪ *Recommended*: Yes ▪ *Examples*: 40 hours annually (may include mentoring, shadowing, conferences, webinars, or rotations)

Cybersecurity Workforce Capabilities (Example 4)



CYBER INSTRUCTIONAL CURRICULUM DEVELOPER

Click to Return to Work Role List

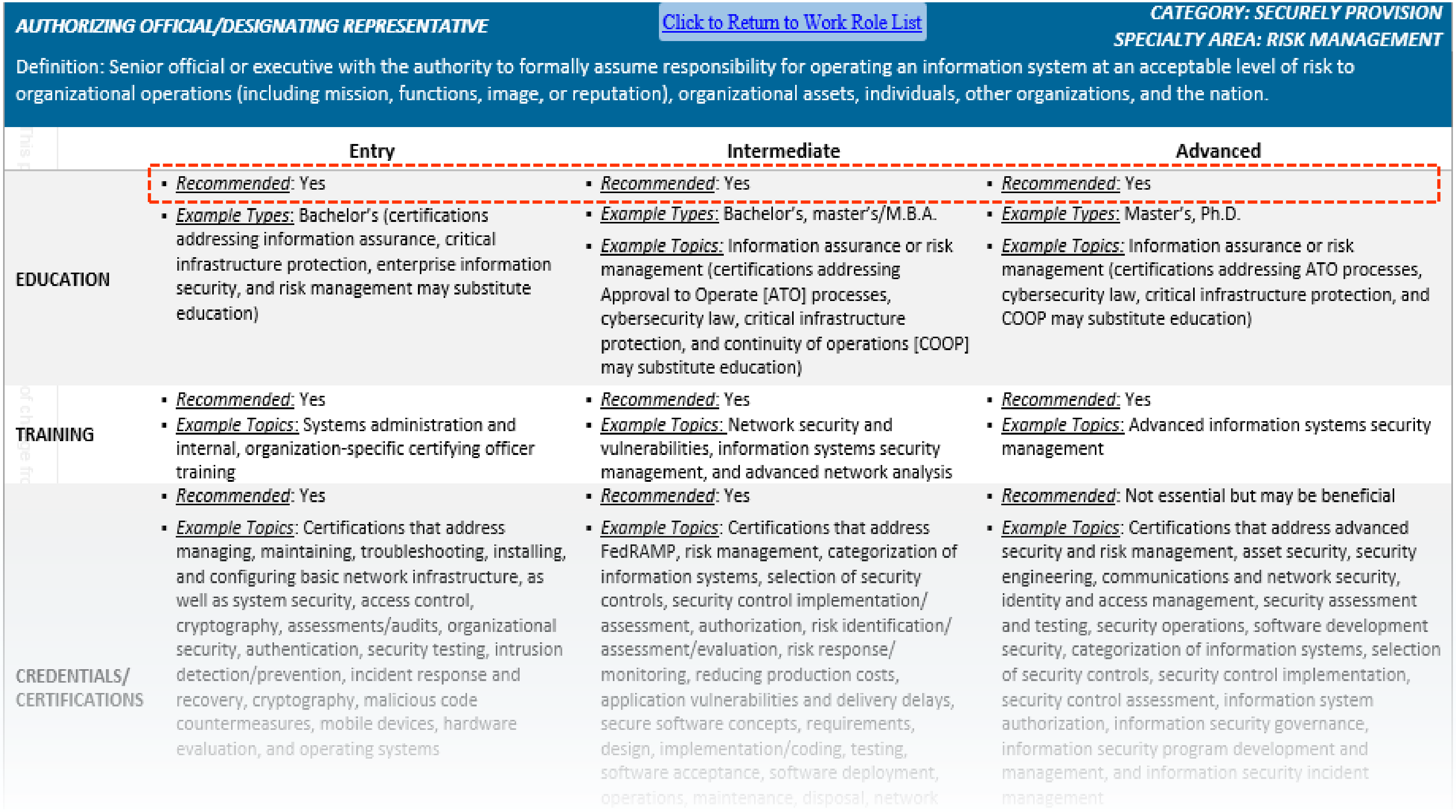
Category: Oversee and Govern
Specialty Area: Training, Education, and Awareness

Definition: Develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs.

Note: For this role, the professional can be a technical expert who has an ability to train (e.g., skill in teaching and being engaging) or can be a skilled trainer who can acquire technical expertise via certifications and hands-on experience.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types:* Associate's, bachelor's ▪ *Example Topics:* Psychology, instructional design, telecommunications, economics, information technology, communications, journalism, information security	▪ *Recommended*: Yes ▪ *Example Types:* Bachelor's ▪ *Example Topics:* Psychology, instructional design, telecommunications, economics, information technology, communications, journalism, information security	▪ *Recommended:* Yes ▪ *Example Types:* Bachelor's, master's, Ph.D. ▪ *Example Topics:* IT, instructional design, information security
TRAINING	▪ *Recommended:* Yes ▪ *Example Topics:* Talent development, human resources, technical, instructional designer, learning, graphic design	▪ *Recommended:* Yes ▪ *Example Topics:* IT, cyber, instructional design, learning, graphic design, vendor (e.g., virtual learning environment and course management system, rapid responsive authoring tools used for creating e-learning content, and online teaching and training software trainings), 508 compliance, learning management systems	▪ *Recommended:* Yes ▪ *Example Topics:* Instructional design, workforce development, learning styles, IT
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: No	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing IT fundamentals, instructional design, training delivery, performance improvement, evaluating learning impact, managing learning programs, coaching, integrated talent management, change management, knowledge management, learning technologies, global mindset, foundational instructional design theories, application(s) for developing learning experiences for digital platforms	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development
EXPERIENTIAL LEARNING	▪ *Recommended*: No	▪ *Recommended*: Yes (Navy data does not recommend) ▪ *Examples*: 2–3 years of hands-on experience, internship, instructional designer frameworks, 508 training, evaluative concepts, adult learning styles, learning cycles, cyber or tech curriculum development experience prior	▪ *Recommended*: Yes ▪ *Examples*: 5–7+ years of hands-on experience including internships, instructional designer frameworks, 508 compliance training, evaluative concepts, exposure to different types of audiences and learning styles,

Cybersecurity Workforce Capabilities (Example 5)



AUTHORIZING OFFICIAL/DESIGNATING REPRESENTATIVE

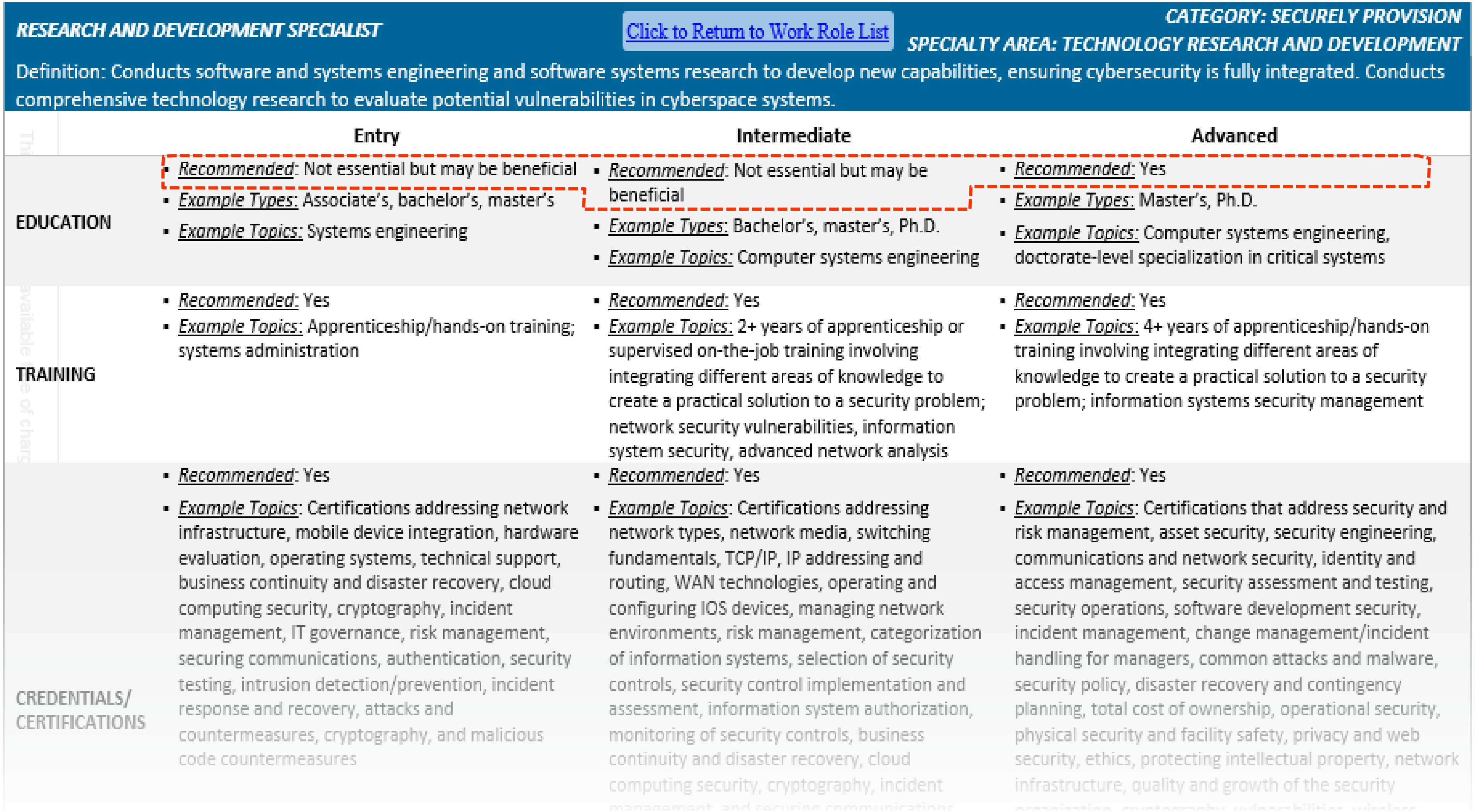
Click to Return to Work Role List

CATEGORY: SECURELY PROVISION
SPECIALTY AREA: RISK MANAGEMENT

Definition: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the nation.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Yes ▪ *Example Types:* Bachelor's (certifications addressing information assurance, critical infrastructure protection, enterprise information security, and risk management may substitute education)	▪ *Recommended*: Yes ▪ *Example Types:* Bachelor's, master's/M.B.A. ▪ *Example Topics:* Information assurance or risk management (certifications addressing Approval to Operate [ATO] processes, cybersecurity law, critical infrastructure protection, and continuity of operations [COOP] may substitute education)	▪ *Recommended:* Yes ▪ *Example Types:* Master's, Ph.D. ▪ *Example Topics:* Information assurance or risk management (certifications addressing ATO processes, cybersecurity law, critical infrastructure protection, and COOP may substitute education)
TRAINING	▪ *Recommended:* Yes ▪ *Example Topics:* Systems administration and internal, organization-specific certifying officer training	▪ *Recommended:* Yes ▪ *Example Topics:* Network security and vulnerabilities, information systems security management, and advanced network analysis	▪ *Recommended:* Yes ▪ *Example Topics:* Advanced information systems security management
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address managing, maintaining, troubleshooting, installing, and configuring basic network infrastructure, as well as system security, access control, cryptography, assessments/audits, organizational security, authentication, security testing, intrusion detection/prevention, incident response and recovery, cryptography, malicious code countermeasures, mobile devices, hardware evaluation, and operating systems	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address FedRAMP, risk management, categorization of information systems, selection of security controls, security control implementation/ assessment, authorization, risk identification/ assessment/evaluation, risk response/ monitoring, reducing production costs, application vulnerabilities and delivery delays, secure software concepts, requirements, design, implementation/coding, testing, software acceptance, software deployment, operations, maintenance, disposal, network	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications that address advanced security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, categorization of information systems, selection of security controls, security control implementation, security control assessment, information system authorization, information security governance, information security program development and management, and information security incident management

Cybersecurity Workforce Capabilities (Example 6)



RESEARCH AND DEVELOPMENT SPECIALIST

Click to Return to Work Role List

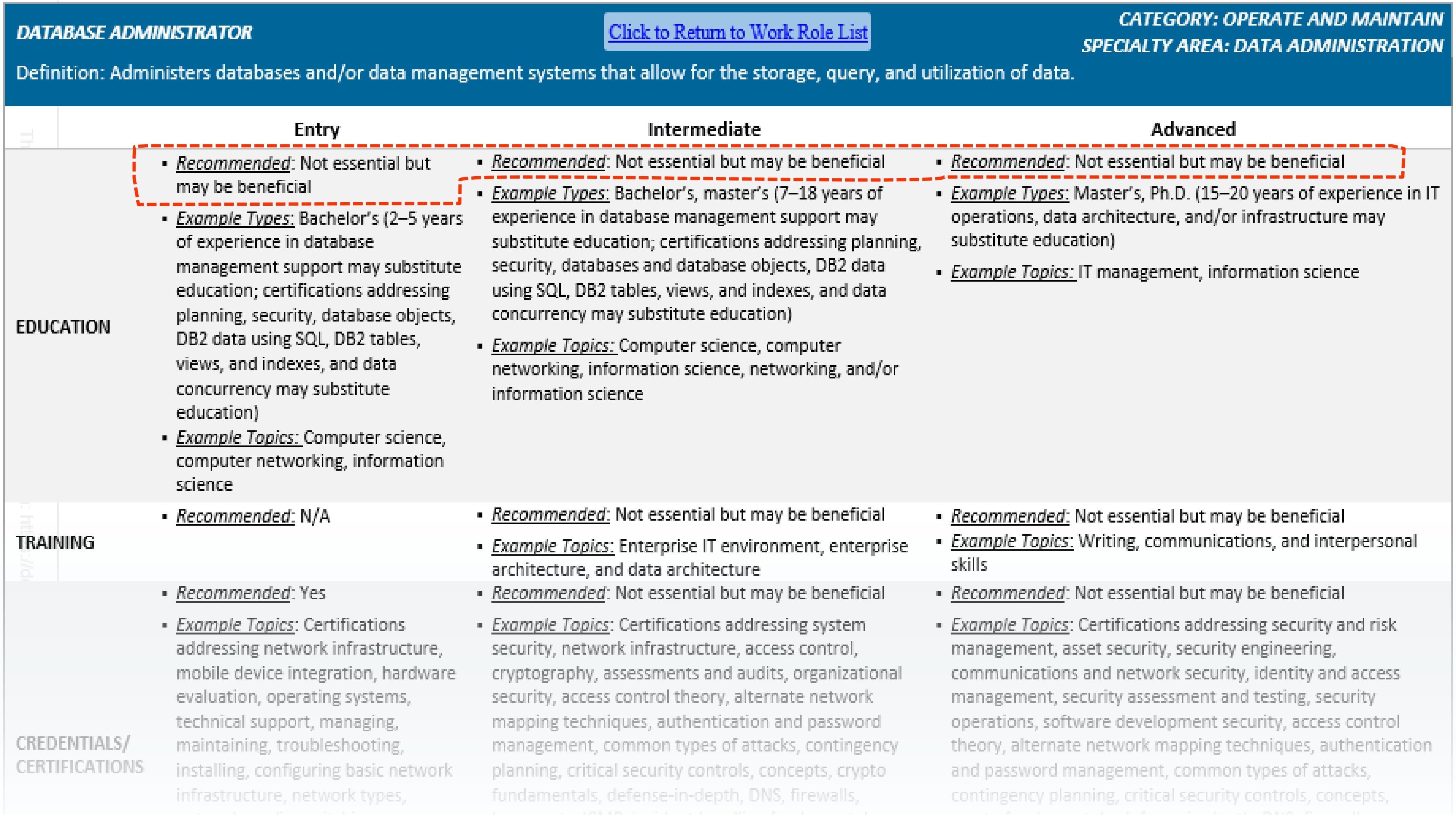
CATEGORY: SECURELY PROVISION

SPECIALTY AREA: TECHNOLOGY RESEARCH AND DEVELOPMENT

Definition: Conducts software and systems engineering and software systems research to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types:* Associate's, bachelor's, master's ▪ *Example Topics:* Systems engineering	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types:* Bachelor's, master's, Ph.D. ▪ *Example Topics:* Computer systems engineering	▪ *Recommended:* Yes ▪ *Example Types:* Master's, Ph.D. ▪ *Example Topics:* Computer systems engineering, doctorate-level specialization in critical systems
TRAINING	▪ *Recommended:* Yes ▪ *Example Topics:* Apprenticeship/hands-on training; systems administration	▪ *Recommended:* Yes ▪ *Example Topics:* 2+ years of apprenticeship or supervised on-the-job training involving integrating different areas of knowledge to create a practical solution to a security problem; network security vulnerabilities, information system security, advanced network analysis	▪ *Recommended:* Yes ▪ *Example Topics:* 4+ years of apprenticeship/hands-on training involving integrating different areas of knowledge to create a practical solution to a security problem; information systems security management
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, business continuity and disaster recovery, cloud computing security, cryptography, incident management, IT governance, risk management, securing communications, authentication, security testing, intrusion detection/prevention, incident response and recovery, attacks and countermeasures, cryptography, and malicious code countermeasures	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing network types, network media, switching fundamentals, TCP/IP, IP addressing and routing, WAN technologies, operating and configuring IOS devices, managing network environments, risk management, categorization of information systems, selection of security controls, security control implementation and assessment, information system authorization, monitoring of security controls, business continuity and disaster recovery, cloud computing security, cryptography, incident management, and securing communications	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications that address security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, incident management, change management/incident handling for managers, common attacks and malware, security policy, disaster recovery and contingency planning, total cost of ownership, operational security, physical security and facility safety, privacy and web security, ethics, protecting intellectual property, network infrastructure, quality and growth of the security organization, cryptography, vulnerabilities, wireless

Cybersecurity Workforce Capabilities (Example 7)



DATABASE ADMINISTRATOR

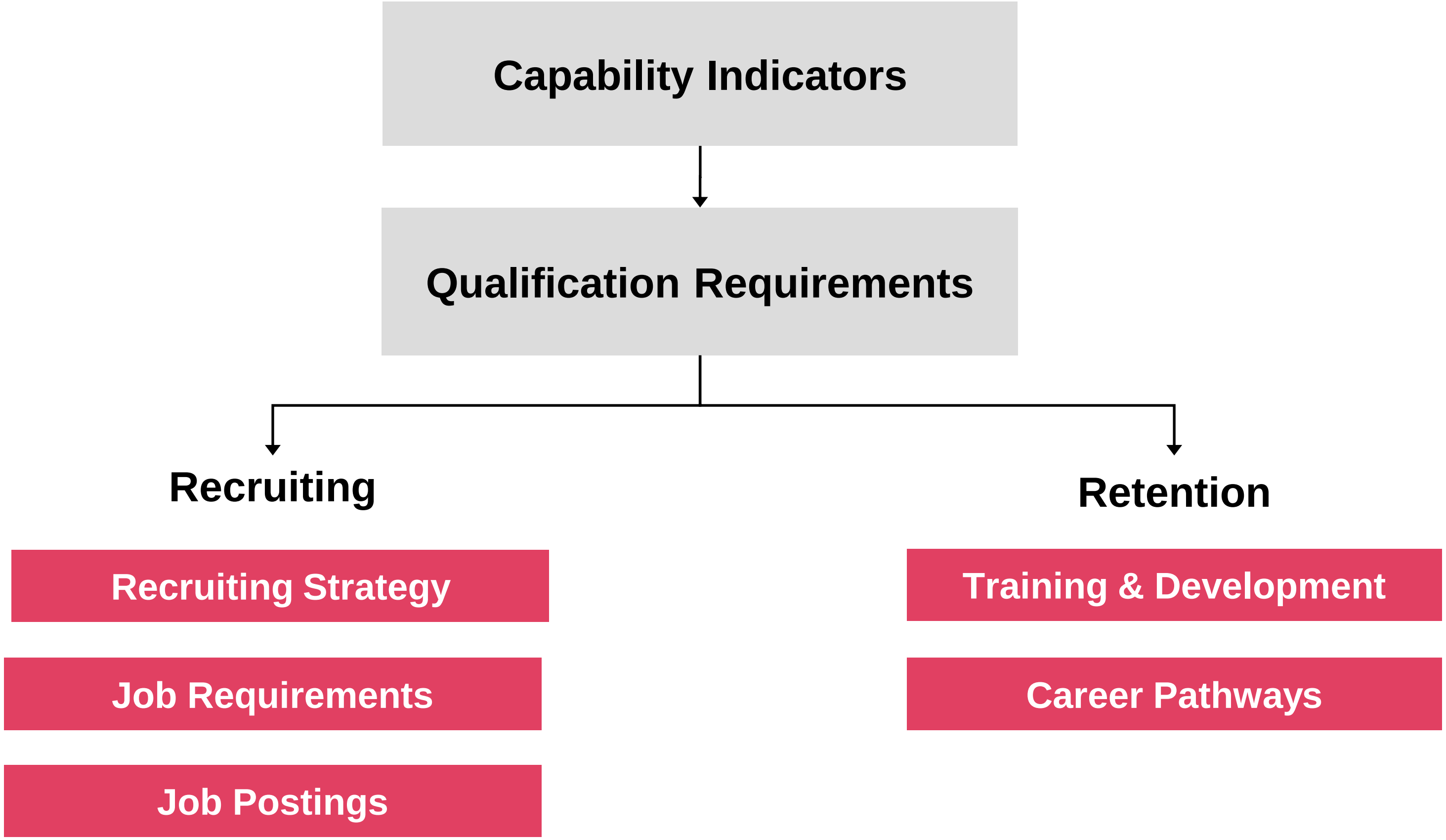
Click to Return to Work Role List

CATEGORY: OPERATE AND MAINTAIN
SPECIALTY AREA: DATA ADMINISTRATION

Definition: Administers databases and/or data management systems that allow for the storage, query, and utilization of data.

	Entry	Intermediate	Advanced
EDUCATION	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types:* Bachelor's (2–5 years of experience in database management support may substitute education; certifications addressing planning, security, database objects, DB2 data using SQL, DB2 tables, views, and indexes, and data concurrency may substitute education) ▪ *Example Topics:* Computer science, computer networking, information science	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types:* Bachelor's, master's (7–18 years of experience in database management support may substitute education; certifications addressing planning, security, databases and database objects, DB2 data using SQL, DB2 tables, views, and indexes, and data concurrency may substitute education) ▪ *Example Topics:* Computer science, computer networking, information science, networking, and/or information science	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Types:* Master's, Ph.D. (15–20 years of experience in IT operations, data architecture, and/or infrastructure may substitute education) ▪ *Example Topics:* IT management, information science
TRAINING	▪ *Recommended:* N/A	▪ *Recommended:* Not essential but may be beneficial ▪ *Example Topics:* Enterprise IT environment, enterprise architecture, and data architecture	▪ *Recommended:* Not essential but may be beneficial ▪ *Example Topics:* Writing, communications, and interpersonal skills
CREDENTIALS/ CERTIFICATIONS	▪ *Recommended*: Yes ▪ *Example Topics*: Certifications addressing network infrastructure, mobile device integration, hardware evaluation, operating systems, technical support, managing, maintaining, troubleshooting, installing, configuring basic network infrastructure, network types,	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing system security, network infrastructure, access control, cryptography, assessments and audits, organizational security, access control theory, alternate network mapping techniques, authentication and password management, common types of attacks, contingency planning, critical security controls, concepts, crypto fundamentals, defense-in-depth, DNS, firewalls,	▪ *Recommended*: Not essential but may be beneficial ▪ *Example Topics*: Certifications addressing security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, software development security, access control theory, alternate network mapping techniques, authentication and password management, common types of attacks, contingency planning, critical security controls, concepts,

Applications for Capability Indicators



Capability Indicators

Qualification Requirements

Recruiting

- Recruiting Strategy
- Job Requirements
- Job Postings

Retention

- Training & Development
- Career Pathways

Submit Your Input

We welcome your feedback on the Work Role Capability Indicators!

Directions

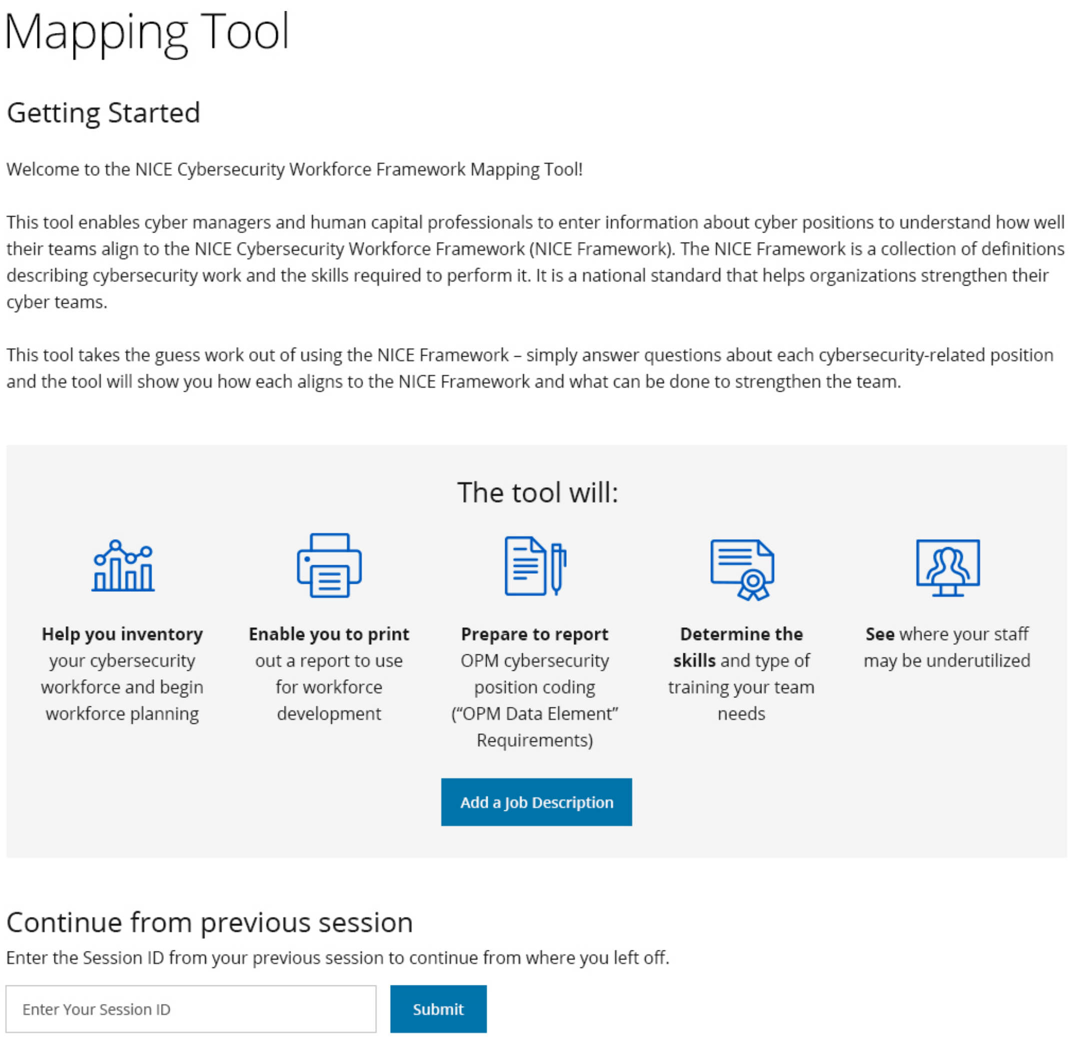
1. The Work Role Capability Indicators are being released for public comment on November 8 in the form of NIST Interagency Report (NISTIR) 8193. You can find the full report at: https://doi.org/10.6028/NIST.IR.8193
2. After carefully reviewing the report, please submit any feedback to cybersecurityworkforce@hq.dhs.gov

Workforce Development Toolkit and Tools

WORKFORCE DEVELOPMENT TOOLKIT PHASES

WORKFORCE DEVELOPMENT TOOLKIT PHASES		TOOLS
PREPARE	‣ Assess goals ‣ Evaluate readiness	○ Workforce Planning Capability Maturity Model (CMM)
PLAN	‣ Inventory workforce ‣ Ongoing workforce planning	○ Cybersecurity Workforce Planning Diagnostic ○ NICE Framework
BUILD	‣ Close skill gaps ‣ Recruit for key skills	○ Team Traits / Interview Questions ○ Recruitment Checklist ○ NICCS Training Catalog
ADVANCE	‣ Retain staff ‣ Provide continuous development	○ Retention Tips by Level ○ Career Path Template

Mapping Tool Homepage



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 guess work 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.

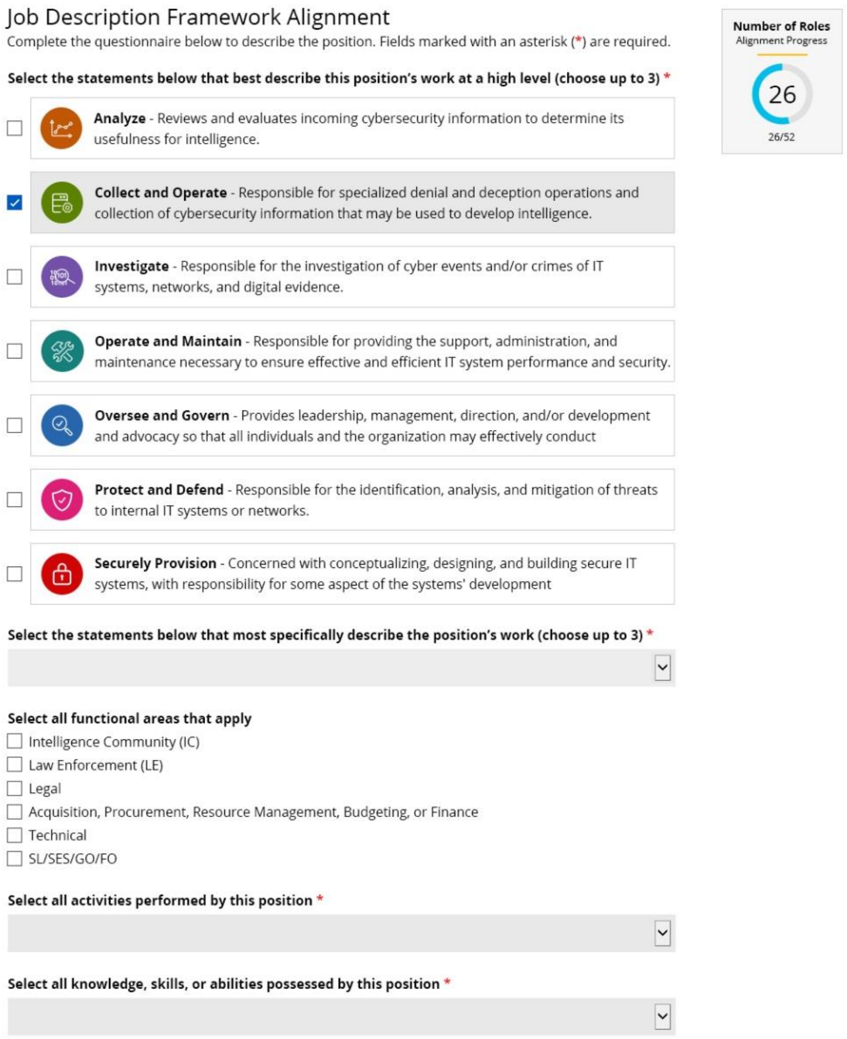
The tool will:

- **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 ("OPM 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.

Mapping Tool: Job Description Submission



Job Description Framework Alignment

Complete the questionnaire 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.

☐ **Oversee 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

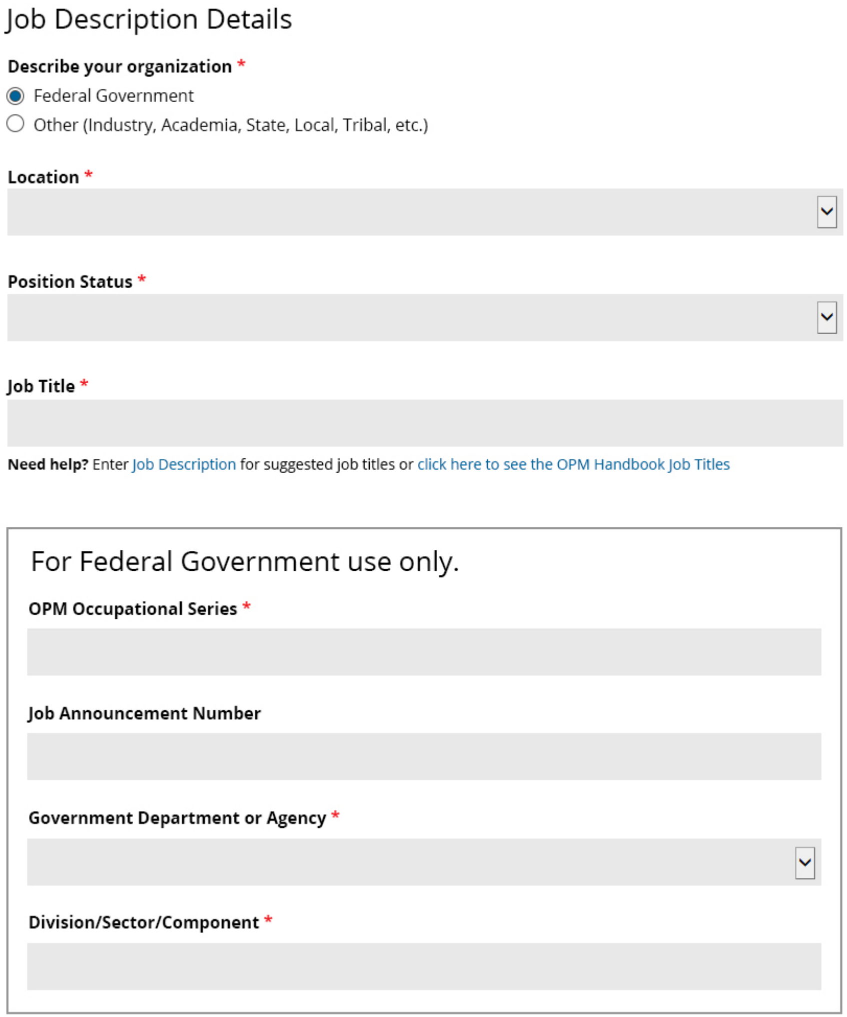
☐ Intelligence Community (IC)
☐ Law Enforcement (LE)
☐ Legal
☐ Acquisition, Procurement, Resource Management, Budgeting, or Finance
☐ Technical
☐ SL/SES/GO/FO

Select all activities performed by this position *

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

Number of Roles
Alignment Progress
26
26/52

Mapping Tool: Job Description Submission



Job Description Details

Describe your organization *

● Federal Government

○ Other (Industry, Academia, State, Local, Tribal, etc.)

Location *

Position Status *

Job Title *

Need help? Enter Job Description for suggested job titles or click here to see the OPM Handbook Job Titles

For Federal Government use only.

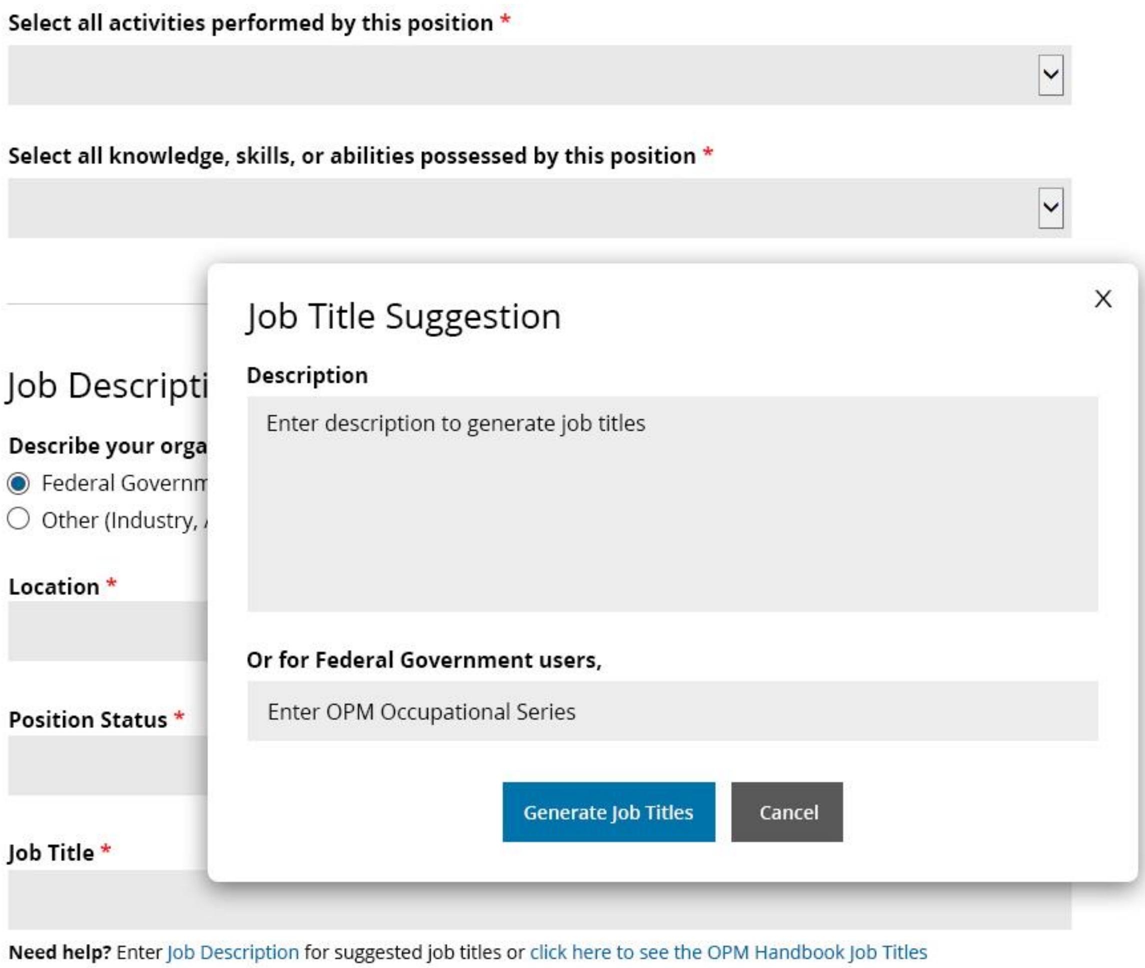
OPM Occupational Series *

Job Announcement Number

Government Department or Agency *

Division/Sector/Component *

Mapping Tool: Job Title Suggestion



Select all activities performed by this position *

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

Job Descripti

Describe your orga

● Federal Governm

○ Other (Industry, /

Location *

Position Status *

Job Title *

Need help? Enter Job Description for suggested job titles or click here to see the OPM Handbook Job Titles

Job Title Suggestion

Description

Enter description to generate job titles

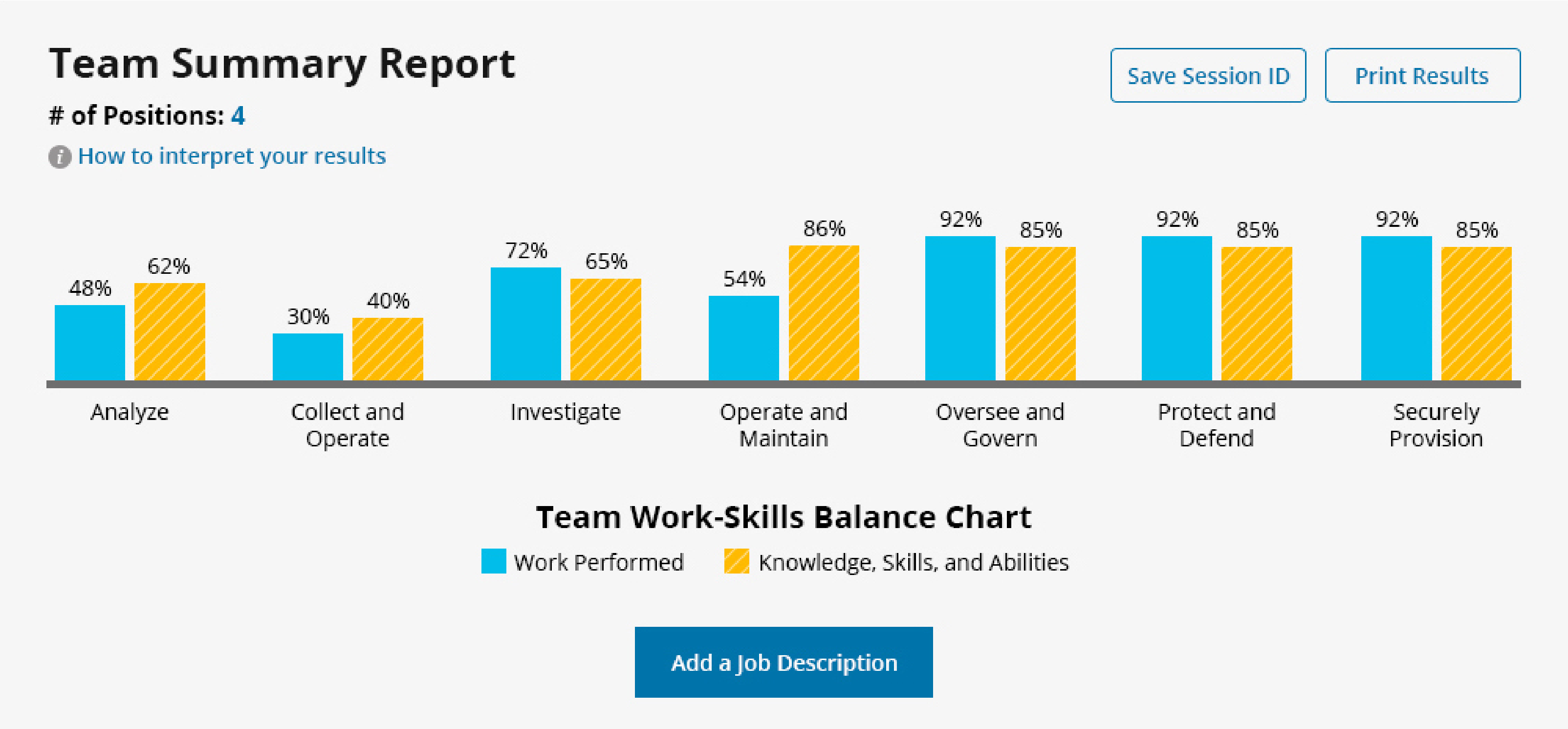
Or for Federal Government users,

Enter OPM Occupational Series

Mapping Tool Report

When you have completed your first position you will see a summary of your results below. The top section is an overall team summary for all of the positions you have entered. Below the Team Summary you will see individual panels for each position. Click on the panel to expand it and see a summary for that position. From this view you can perform the following actions:

- **View Details** – View a complete listing of the position and its alignment to the Workforce Framework.
- **Update Position** – Modify the information for this position.
- **Remove Position** – Remove this position from your assessment.

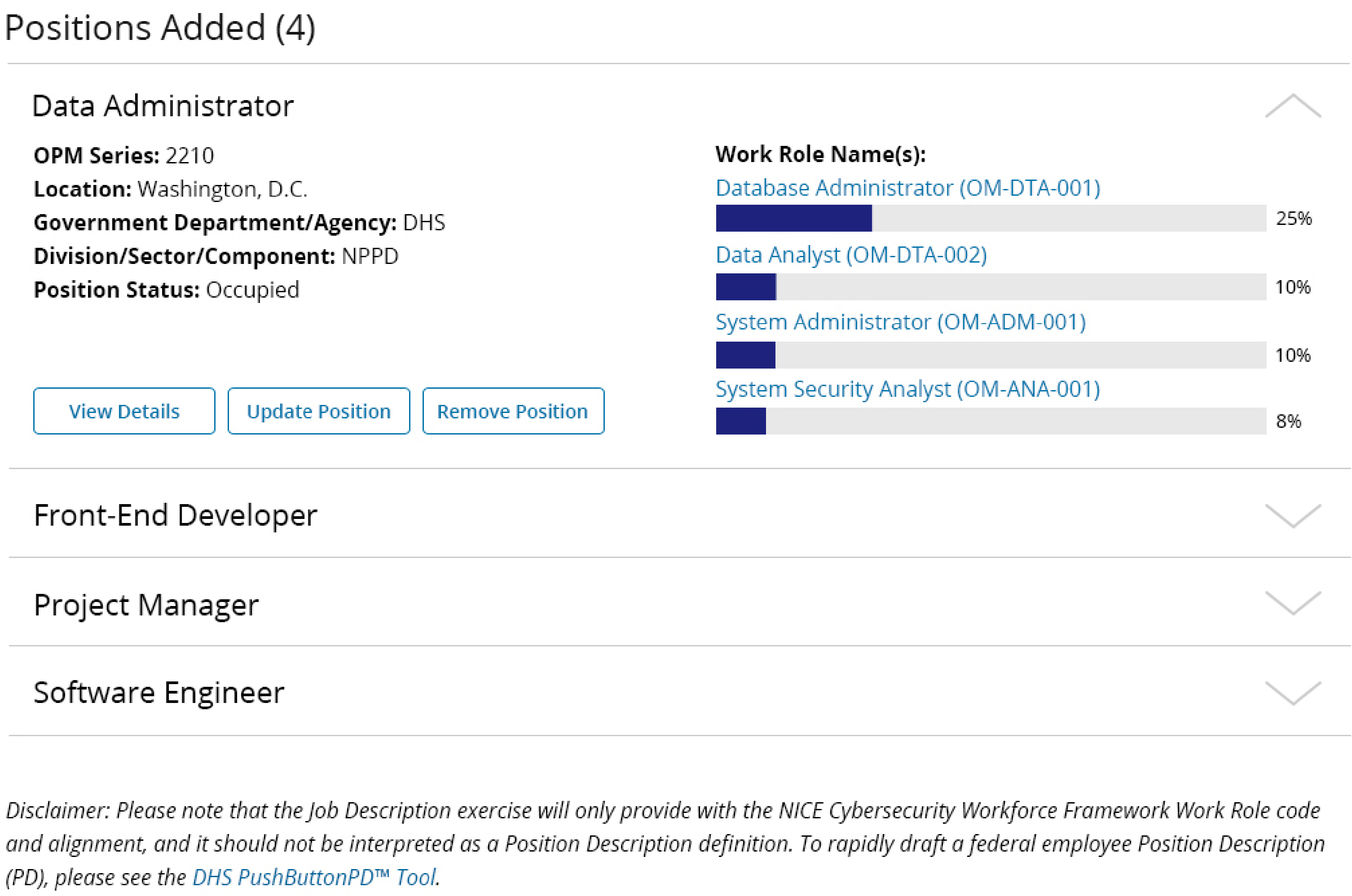


Team Summary Report

# of Positions: 4

How to interpret your results

Mapping Tool Report: Position Details



Positions Added (4)

Data Administrator

OPM Series: 2210
Location: Washington, D.C.
Government Department/Agency: DHS
Division/Sector/Component: NPPD
Position Status: Occupied

Work Role Name(s):

Database Administrator (OM-DTA-001) 25%

Data Analyst (OM-DTA-002) 10%

System Administrator (OM-ADM-001) 10%

System Security Analyst (OM-ANA-001) 8%

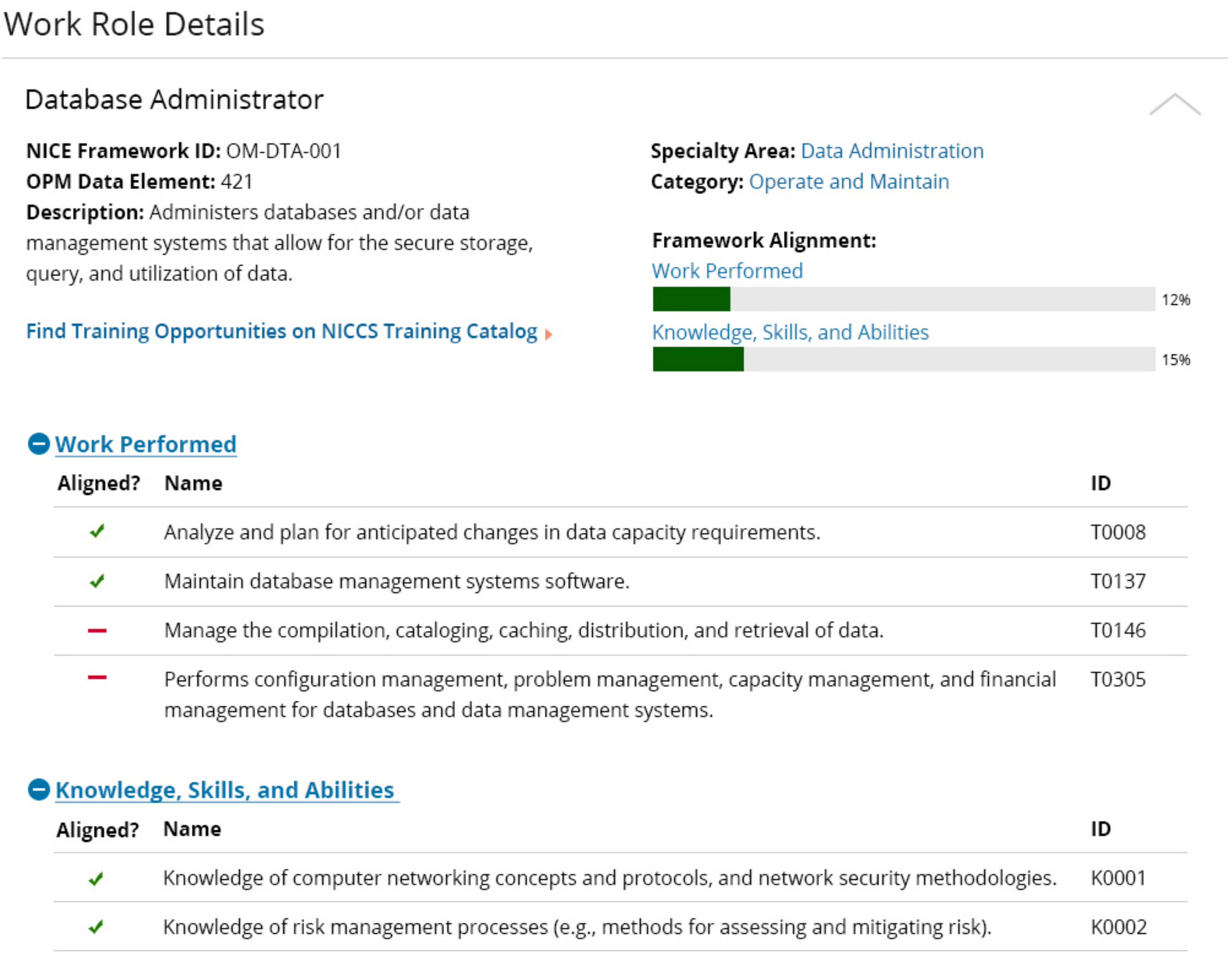
Front-End Developer

Project Manager

Software Engineer

Disclaimer: Please note that the Job Description exercise will only provide with the NICE Cybersecurity Workforce Framework Work Role code and alignment, and it should not be interpreted as a Position Description definition. To rapidly draft a federal employee Position Description (PD), please see the DHS PushButtonPD™ Tool.

Mapping Tool Report: Position Details



Work Role Details

Database Administrator

NICE Framework ID: OM-DTA-001
OPM Data Element: 421
Description: Administers databases and/or data management systems that allow for the secure storage, query, and utilization of data.

Find Training Opportunities on NICCS Training Catalog ▸

Specialty Area: Data Administration
Category: Operate and Maintain

Framework Alignment:

Work Performed 12%

Knowledge, Skills, and Abilities 15%

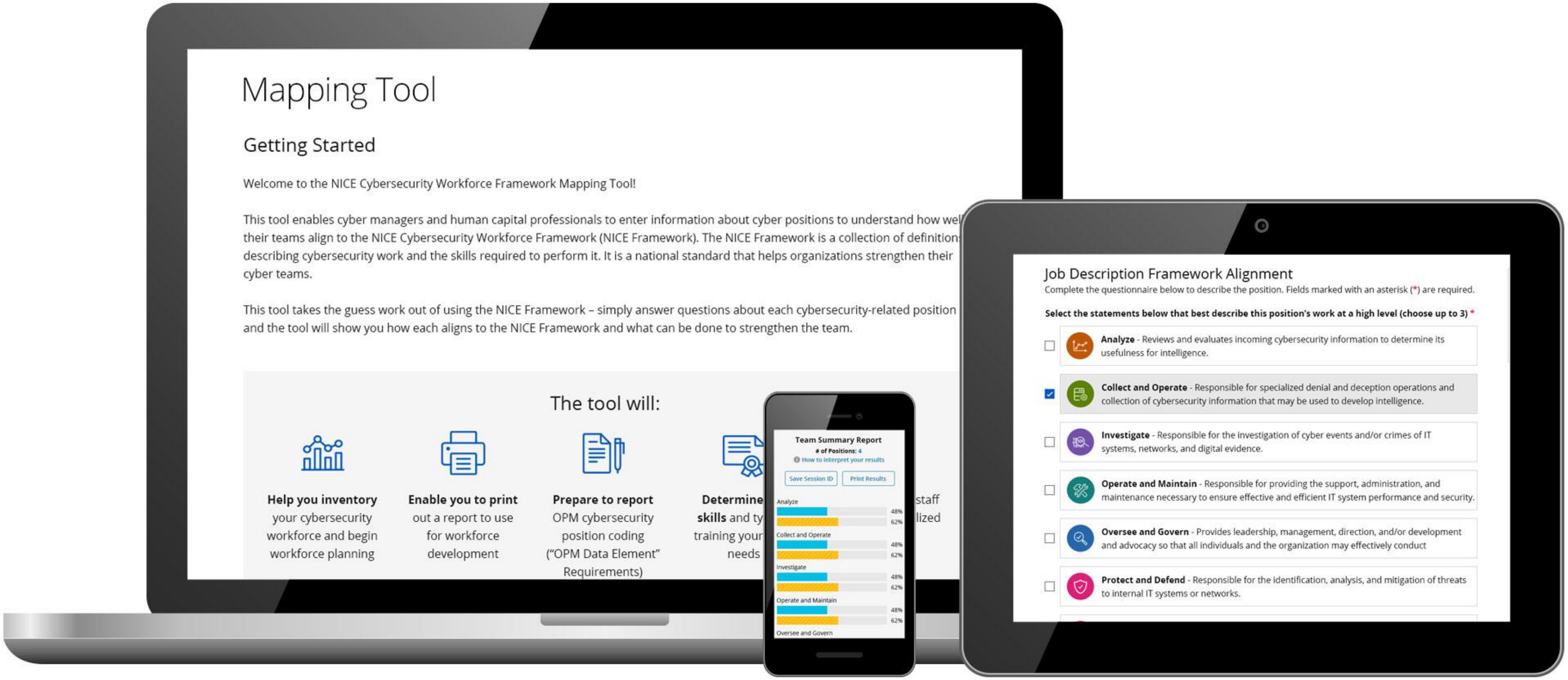
Work Performed

Aligned?	Name	ID
✓	Analyze and plan for anticipated changes in data capacity requirements.	T0008
✓	Maintain database management systems software.	T0137
—	Manage the compilation, cataloging, caching, distribution, and retrieval of data.	T0146
—	Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.	T0305

Knowledge, Skills, and Abilities

Aligned?	Name	ID
✓	Knowledge of computer networking concepts and protocols, and network security methodologies.	K0001
✓	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	K0002

Mapping Tool Website



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 wel their teams align to the NICE Cybersecurity Workforce Framework (NICE Framework). The NICE Framework is a collection of definition 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 guess work 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 ("OPM Data Element" Requirements)
- **Determine skills** and ty training your needs
- staff lized

Team Summary Report

# of Positions: 4

How to interpret your results

Save Session ID | Print Results

Job Description Framework Alignment

Complete the questionnaire below to describe the position. Fields marked with an asterisk (*) are required.

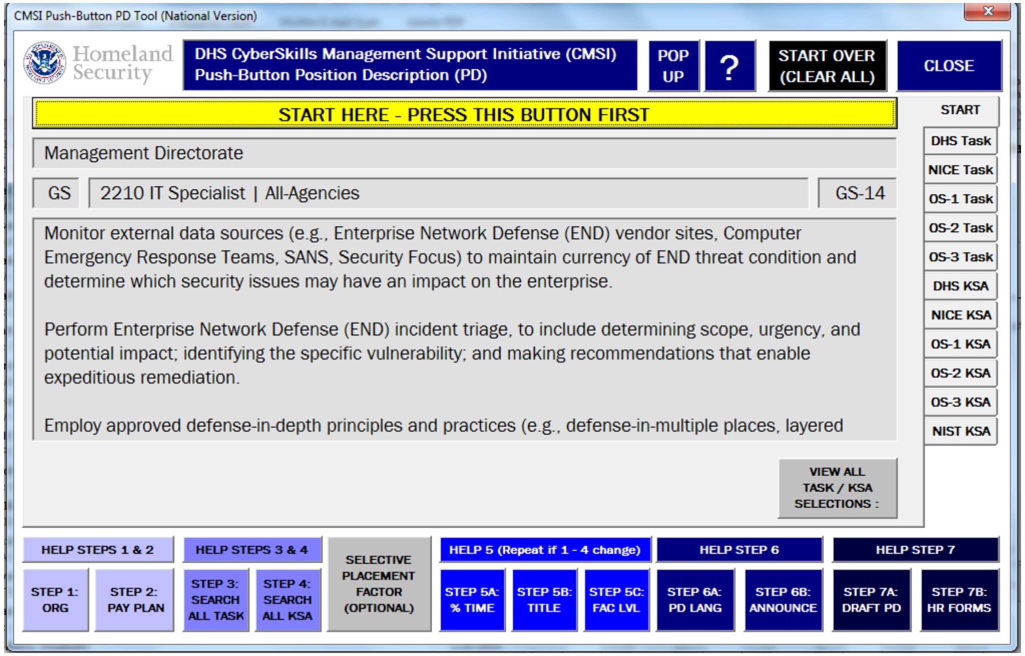
Select the statements below that best describe this position's work at a high level (choose up to 3) *

- ☐ **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.
- ☐ **Oversee 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.

https://niccs.us-cert.gov

DHS PushButton PD™ Tool

- Generates Cyber and non-Cyber federal employee Position Description (PD) drafts
- Pre-loaded with Task and KSA language
- Automatically recommends NICE Framework data elements
- Produces optional HR forms such as Job Analysis worksheets



Management Directorate

GS | 2210 IT Specialist | All-Agencies | GS-14

Monitor external data sources (e.g., Enterprise Network Defense (END) vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of END threat condition and determine which security issues may have an impact on the enterprise.

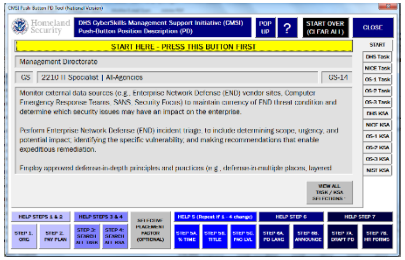
Perform Enterprise Network Defense (END) incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation.

Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered

https://niccs.us-cert.gov/workforce-development/dhs-pushbuttonpd-tool

DHS PushButton PD™ Tool

MAIN INTERFACE:



Management Directorate

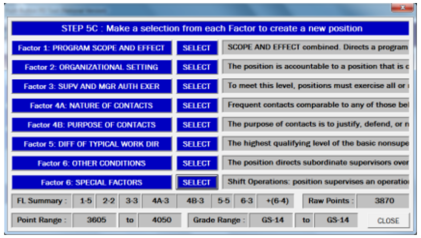
GS | 2210 IT Specialist | All-Agencies | GS-14

Monitor external data sources (e.g., Enterprise Network Defense (END) vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of END threat condition and determine which security issues may have an impact on the enterprise.

Perform Enterprise Network Defense (END) incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation.

Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered

SUPERVISORY FACTOR LEVEL MENU:



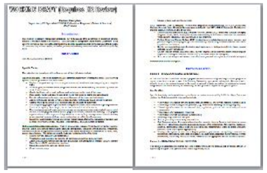
STEP 5C : Make a selection from each Factor to create a new position

Factor 1: PROGRAM SCOPE AND EFFECT	SCOPE AND EFFECT combined. Directs a program
Factor 2: ORGANIZATIONAL SETTING	The position is accountable to a position that is c
Factor 3: SUPV AND MGR AUTH EXER	To meet this level, positions must exercise all or
Factor 4A: NATURE OF CONTACTS	Frequent contacts comparable to any of those bel
Factor 4B: PURPOSE OF CONTACTS	The purpose of contacts is to justify, defend, or n
Factor 5: DIFF OF TYPICAL WORK DIR	The highest qualifying level of the basic nonsupe
Factor 6: OTHER CONDITIONS	The position directs subordinate supervisors over
Factor 6: SPECIAL FACTORS	Shift Operations: position supervises an operatio

FL Summary : 1-5 | 2-2 | 3-3 | 4A-3 | 4B-3 | 5-5 | 6-3 | +(6-4) — Raw Points : 3870

Point Range : 3605 to 4050 — Grade Range : GS-14 to GS-14

POSITION DESCRIPTION OUTPUT:



- ***PushButtonPD*** is a no-cost, self-contained, single Excel workbook file currently under 3 MB.
- Managers, supervisors, and HR Specialists can rapidly draft Position Descriptions (PDs) without the need for extensive training or prior knowledge of position classification.
- It is designed to present language from multiple authoritative sources and standards for duty, task, and KSAs (knowledge, skills, and abilities); rapidly capture the hiring official’s requirements; and present them in a package that can be easily integrated into the agency’s current HR processes.
- The entire PD generation timeline becomes a process that can be completed, not in weeks/months, but in a matter of days/weeks.

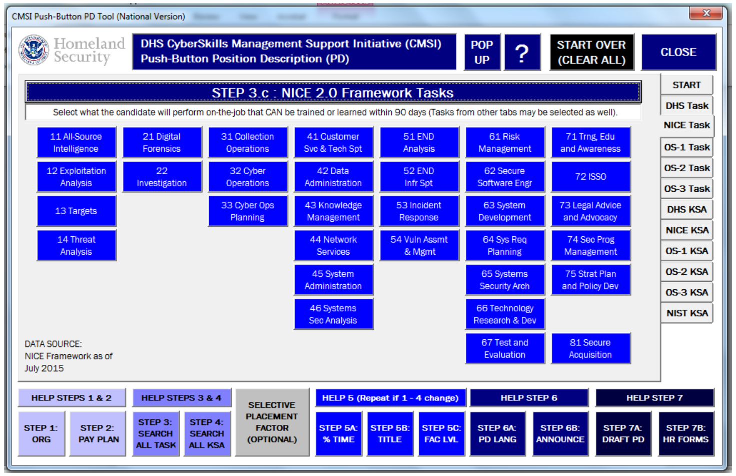
NICE Task Tab

- **Integrated Capability**. Originally built from the ground-up to support cyberskill-related Occupational Series and expanded later to accommodate other series.
- **NICE Framework:** Assigns NICE Framework code according to Major Duty (or a general code when minor duties comprise 25% or more of duties)
- **Integrated Task and KSA Standards**: DHS HSAC Mission-Critical Tasks and NICE 2.0 (Draft) Framework Tasks and Knowledge, Skills, and Abilities (KSAs); OPM MOSAIC KSAs

Customization: Editable text (templates or output) and can customize towards organization-specific requirements without tech support.

Security: Processed through Agency's normal security process for Excel-based VB macro worksheets. Digitally signed by the program author.

NICE TASK TAB



CMSI Push-Button PD Tool (National Version)

DHS CyberSkills Management Support Initiative (CMSI)
Push-Button Position Description (PD)

STEP 3.c : NICE 2.0 Framework Tasks

Select what the candidate will perform on-the-job that CAN be trained or learned within 90 days (Tasks from other tabs may be selected as well).

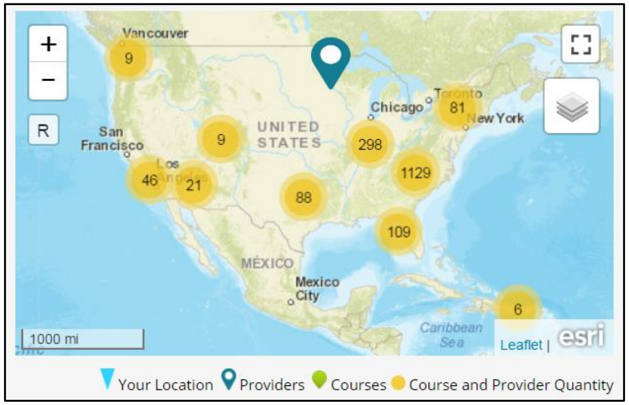
DATA SOURCE:
NICE Framework as of
July 2015

Access to Training and other Cyber Resources

DHS CE&A resources are easy to access through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Training catalog with thousands of cyber-related courses
- List of upcoming cybersecurity events
- Tools for cyber managers
- Custom searches for cybersecurity positions
- Hundreds of links to cybersecurity resources



niccs.us-cert.gov

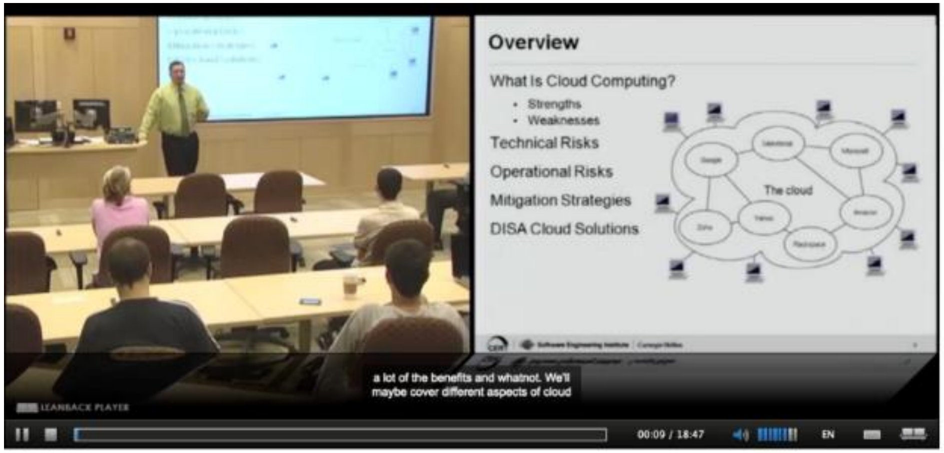
NICCS averages 30,000 users each month

Cybersecurity Training for Veterans

Build and strengthen key knowledge and skills

Federal Virtual Training Environment (FedVTE) offers free, online, 24-hour on-demand training available to U.S. government employees and veterans

Sign up for an account at fedvte.usalearning.gov



Overview

What Is Cloud Computing?

- Strengths
- Weaknesses

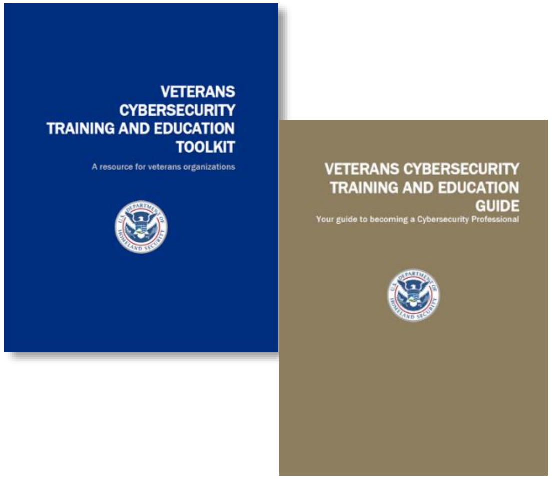
Technical Risks

Operational Risks

Mitigation Strategies

DISA Cloud Solutions

The cloud
a lot of the benefits and whatnot. We'll maybe cover different aspects of cloud
LEANBACK PLAYER
00:09 / 18:47
EN



VETERANS CYBERSECURITY TRAINING AND EDUCATION TOOLKIT

A resource for veterans organizations

VETERANS CYBERSECURITY TRAINING AND EDUCATION GUIDE

Your guide to becoming a Cybersecurity Professional

The **Cybersecurity Training and Education Guide** helps veterans:

- Assess if a career in cybersecurity is the right path
- Plan the career transition
- Use DHS training resources

The **Toolkit** provides sample language to connect with veterans

Visit niccs.us-cert.gov/training/veterans to download the guide and toolkit

Integrating Cybersecurity into the Classroom

Encourage early knowledge and interest

Free Cybersecurity Curriculum funded by DHS

- The **Cybersecurity Education and Training Assistance Program (CETAP) grant** equips teachers with learning tools
- **9 free,** year-long (180 hour) courses plus more modular, project-driven content
- **5,000+ teachers** use the curricula impacting 1.3 million students
- Workshops for teachers and camps for exploring aptitude

Download curricula: nicerc.org

Real-World Application Opportunities

- Consider cyber competitions with real-world scenarios in a competitive environment

  For a full list of competitions, visit: cybercompex.org

Join Stop.Think.Connect.™

DHS is partnering with governments, industry, and academic institutions to raise the level of cyber awareness across the nation.

Stop.Think.Connect.™ provides tools and information so all digital citizens stay safer and more secure online.

- 400+ partners across all sectors and in 50 states
- 115+ colleges/universities have joined The Academic Alliance program
- 40,000+ *Friends* of the Campaign
- 165+ members in the Cyber Awareness Coalition

STOP | THINK | CONNECT™

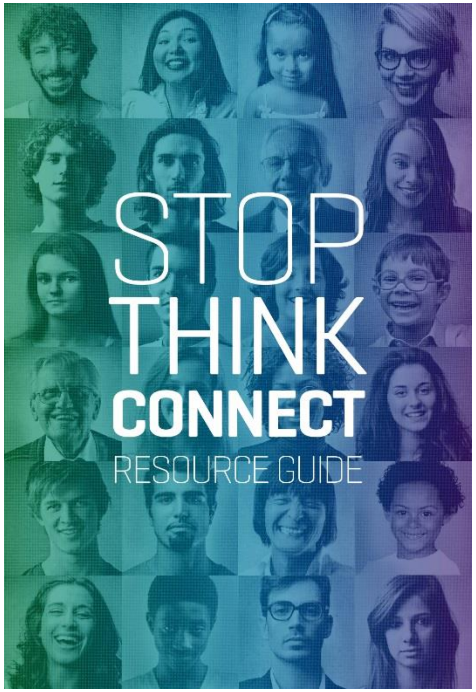
Stop.Think.Connect. Resources

The Campaign provides **FREE** resources available to the public, with toolkit materials designed for a wide variety of audiences.

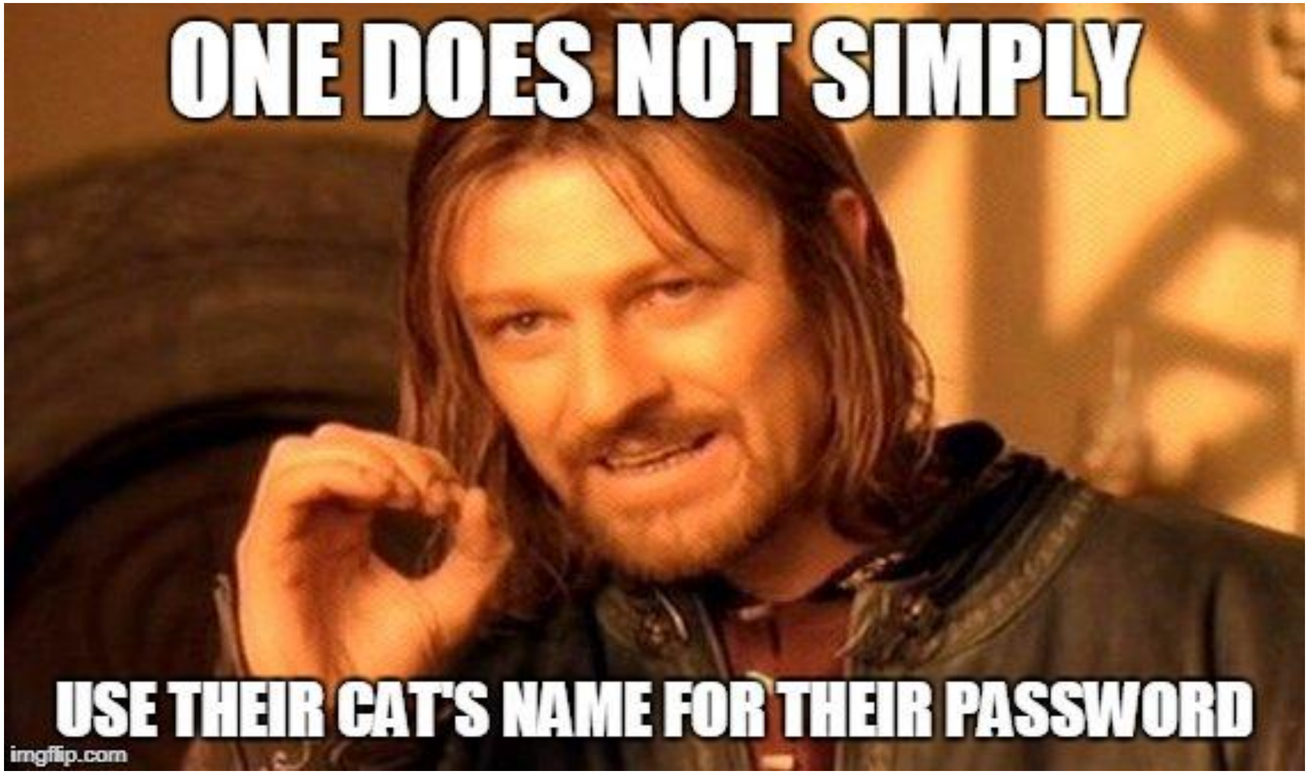
✓ **Download materials (**posters, presentations, and tip sheets) covering topics including:

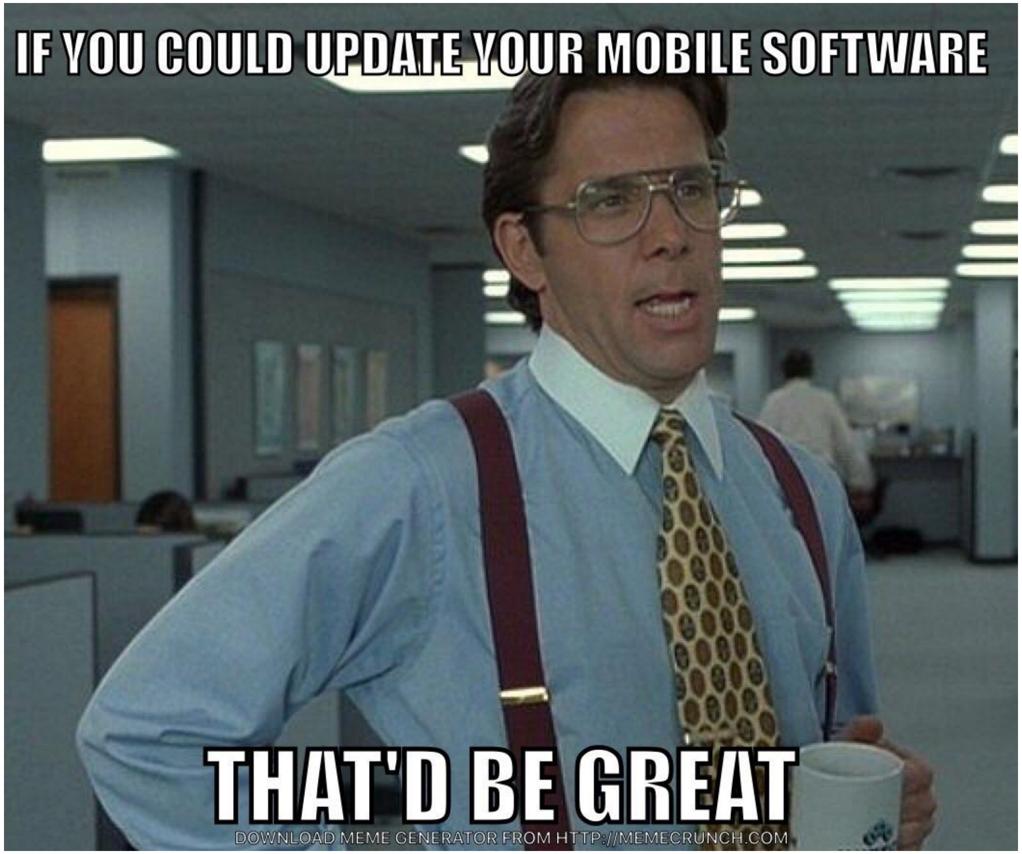
- Online safety for kids
- Mobile security
- Social Media and Online Privacy
- Phishing and Identify Theft
- Malware

✓ **Share resources** with your colleagues, family, and community



Download @
www.dhs.gov/stopthinkconnect


ONE DOES NOT SIMPLY
USE THEIR CAT'S NAME FOR THEIR PASSWORD
imgflip.com

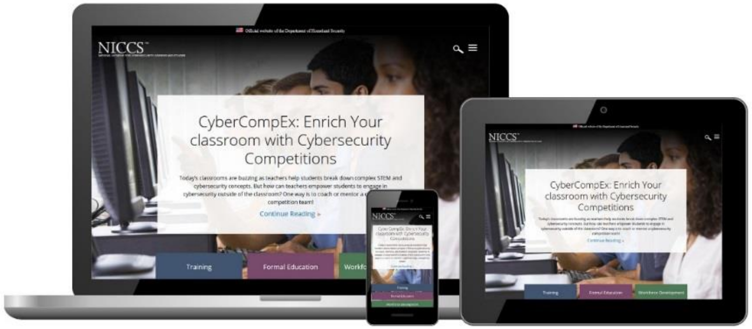

IF YOU COULD UPDATE YOUR MOBILE SOFTWARE
THAT'D BE GREAT
DOWNLOAD MEME GENERATOR FROM HTTP://MEMECRUNCH.COM

THEY STOLE MY IDENTITY
BY USING INFORMATION FROM MY FACEBOOK PAGE
imgflip.com

A Few Best Practices

- Promote NICE Framework adoption
- Align people, as well as positions, to 3 digit Work Role codes
- Leverage NICCS and FedVTE
- Develop career paths aligned to the NICE Framework; encourage employees to build IDPs using Tasks and KSAs
- Get involved!
- Look for NISTIR #8193 at https://doi.org/10.6028/NIST.IR.8193 and provide your input

How to Reach Us



CyberCompEx: Enrich Your classroom with Cybersecurity Competitions

Today's classrooms are buzzing as teachers help students break down complex STEM and cybersecurity concepts. But how can teachers empower students to engage in cybersecurity outside of the classroom? One way is to coach or mentor a c competition team!

Continue Reading »

Noel Kyle

Program Manager

Cybersecurity Education & Awareness

Phone: (202) 815-7837

Email: niccs@hq.dhs.gov

Noel.Kyle@hq.dhs.gov

NICCS: niccs.us-cert.gov