NICE Webinar Series

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Efforts to Align Training and Certifications to the NICE Framework

September 20, 2017

NICE Strategic Goals - https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan

Accelerate Learning and Skills Development

- *Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers*

Nurture A Diverse Learning Community

- *Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce*

Guide Career Development & Workforce Planning

- *Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent*

NICE Strategic Goal #3: Guide Career Development and Workforce Planning

Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent

Objectives:

3.1 Identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers

3.2 Publish and raise awareness of the NICE Cybersecurity Workforce Framework and encourage adoption

3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

3.4 Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals

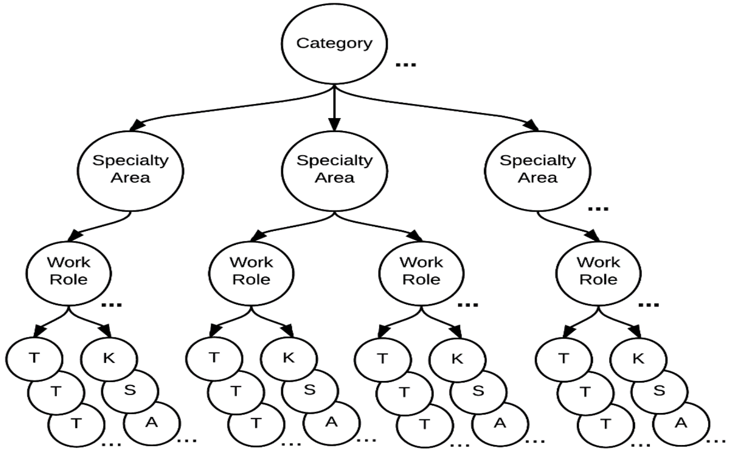
3.5 Collaborate internationally to share best practices in cybersecurity career development and workforce planning

Categories of Cybersecurity Work

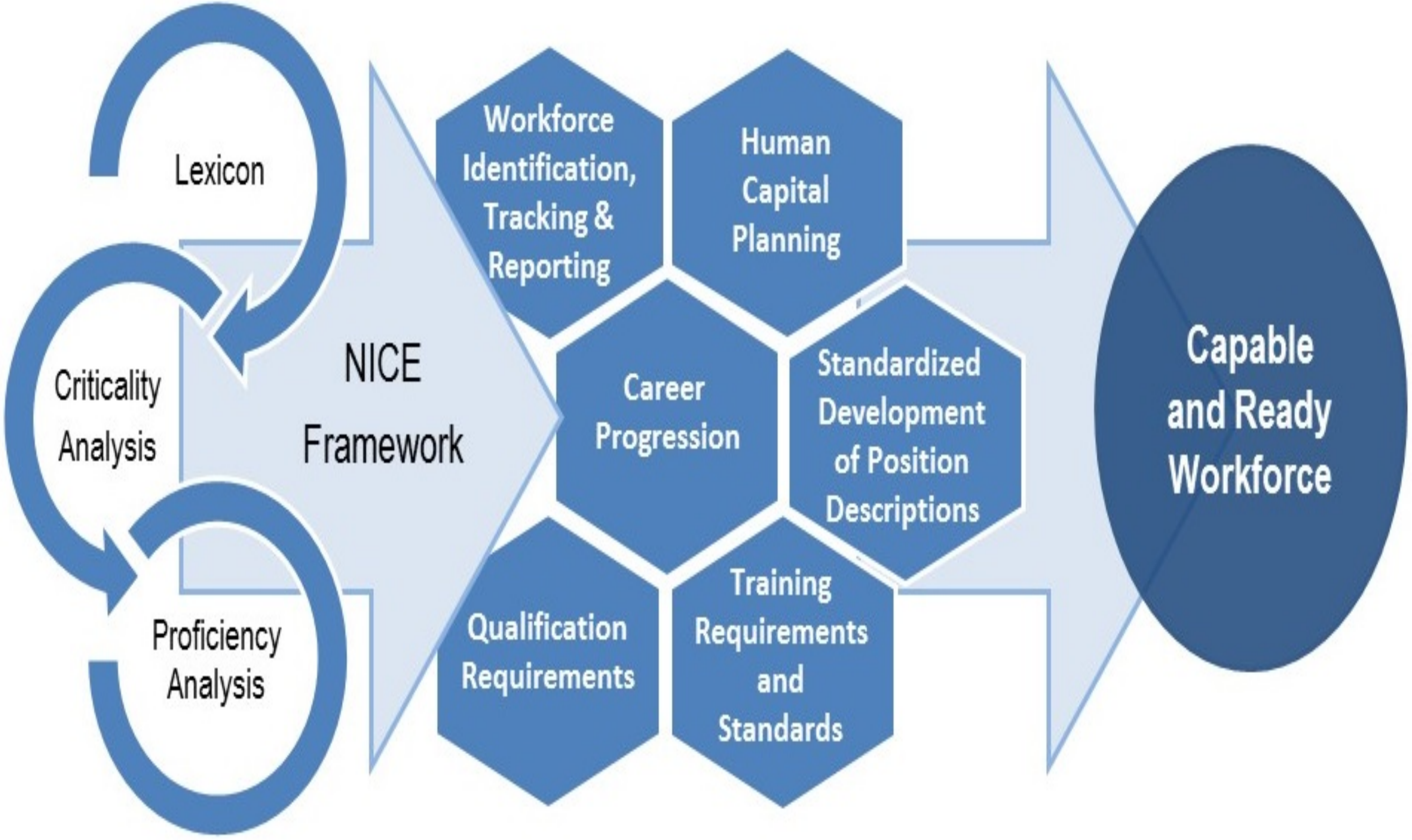
SECURELY PROVISION | OPERATE AND MAINTAIN | OVERSEE AND GOVERN | PROTECT AND DEFEND | ANALYZE | COLLECT AND OPERATE | INVESTIGATE

- Specialty Areas (33) – Distinct areas of cybersecurity work;
  - Work Roles (52) – The most detailed groupings of cybersecurity work, which include specific knowledge, skills, and abilities required to perform a set of tasks.
    - Tasks – Specific work activities that could be assigned to a professional working in one of the NCWF's Work Roles; and,
    - Knowledge, Skills, and Abilities (KSAs) – Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training.

- Audience:
  - Employers
  - Current and Future Cybersecurity Workers
  - Training and Certification Providers
  - Education Providers
  - Technology Providers



Building Blocks for a Capable and Ready Cybersecurity Workforce


Lexicon
Criticality Analysis
Proficiency Analysis
NICE Framework
Workforce Identification, Tracking & Reporting
Human Capital Planning
Career Progression
Standardized Development of Position Descriptions
Qualification Requirements
Training Requirements and Standards
Capable and Ready Workforce

Key Cybersecurity Certifications

Cybersecurity certifications are valuable for anyone in the cybersecurity space, and DHS has a page in their NICCS Portal that has compiled a list of well-known industry certifications at https://niccs.us-cert.gov/featured-stories/cybersecurity-certifications

- Some are perfect starting points on one’s career path
- Others will help increase future career opportunities.

National Initiative for Cybersecurity Education (NICE) – https://nist.gov/nice

- The NICE strategic plan https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan
- The NICE Cybersecurity Workforce Framework https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Resources/Activities (for industry, gov't, and academia)

- The NICE Working Group and subgroups (K-12, Collegiate, Competitions, Training and Certifications, and Workforce Management) https://www.nist.gov/itl/applied-cybersecurity/nice/about/working-group
  - Forum to identify and share best practices that help us as a nation make progress towards the NICE Strategic goals and objectives.
- NICE grants to 5 Regional Alliances and Multistakeholder Partnerships to Stimulate (RAMPS) Cybersecurity Education and Workforce Development
- NICE grant for the creation of Cyberseek http://cyberseek.org/
- NICE challenge Project https://www.nice-challenge.com/
  - cyber challenge labs emphasize real world skills like problem solving, self-learning, and documentation over regurgitating step-by-step instructions and limited simulations.

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Q & A

NICE Framework Mapping Certifications to Roles and Proficiencies

- **NICE Training and Certification Working Group Certification to Roles Effort**
  - **Many certification providers and organizations mapped certifications to the NICE Workforce Framework Version 1 based on standards developed by the organizations**
  - **The team will leverage that work to expand to the new Roles Framework**
  - **Additionally, the team will look to incorporate proficiency level mapping based on the work the NICE Proficiency Team is developing**
  - **Standards will include mapping of tasks and knowledge, skills and abilities along with experience and what is necessary to support attainment of proficiency as the different proficiency levels**
  - **The resulting foundational mapping of certifications will establish a starting point and common understanding of tasks within the workforce**
  - **This effort will also reciprocity across private and public sectors**

Q & A

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Input Derived From: NICE Skills-based Training/Certification Project Team

Description - Skills-based Training/Certification Tiger Team: Build on cyber workforce studies indicating the three most common skill deficiencies are communication skills, business knowledge, and technical skills to provide vendor agnostic skills-based training and performance certification guidelines and tools assisting with problem definition, gap analysis, analytics, and solution sets.

Project Team Members represent: Bellevue University, GIAC, The Herjavec Group, Houston Infragard, ISACA, ISC2, Time Warner, University of South Florida

Presentation Goals / Agenda

- Review basic approach
- Summary of T&C project team topics
- Avoiding ‘can't *see the forest* for the *trees’*
- Some examples of methodology starting points
- Suggested next steps
- Examples from Special Publication 800-181, the NICE Cybersecurity Workforce Framework

Mapping 101

- Derivative work of NICE Skills-based Training/Certification Project Team and many years of Cybersecurity Credentials Collaborative (C3) & member organizations' experience working with industry experts
- Mapping 101 could start with suggestions of what not to do, there is a lot of white space out there
- Correct proficiency ratings and scale are a key to mapping
- KSATs can be looked at from either job fit (baseline vs. variable) or skill level (novice vs. advanced) approach
- Mapping procedure needs to be developed such that any party familiar with the instructional/certification material could apply the mapping and reach a similar mapping conclusion

A Primer on Bloom & Dreyfus Taxonomies

- 1956 committee lead by Benjamin Bloom (Bloom, et al. 1956) that identifies six successive cognitive levels. The intent of these cognitive levels was to classify tasks and knowledges as being less complex (e.g., recall) to more complex (e.g., evaluation). knowledge, comprehension, application, analysis, synthesis, evaluation.
  - As Bloom uses six levels some mapping would be required to align with our three tier proficiency scale. A potential mapping could be entry-level (Knowledge, comprehension, application), intermediate (analysis), advanced (synthesis, evaluation)
- In 1986, Dreyfus and Dreyfus (1986) proposed a skill acquisition model to describe of the acquisition of skill from a novice to expert level of competence. Dreyfus utilizes five levels; novice, advanced beginner, competent, proficient, expert
  - As with Bloom Dreyfus appeared to be of limited use in classifying knowledge, as written all knowledges are potentially at the novice level.
  - Dreyfus potentially seems to be a more applicable taxonomy for defining task and KSA proficiency as related to work roles. Similar to Bloom there would need to be a mapping of these five levels to the three tier proficiency scale. A potential mapping could be entry-level (novice, advanced beginner, competent), intermediate (proficient), advanced (expert).

Taxonomy	Entry-level	Intermediate	Expert
Bloom	Remember Understand	Apply Analyze	Evaluate Create
Dreyfus	Novice Advanced Beginner Competent	Proficient	Expert

Scale and Rating Definitions

- Before conducting homogeneous mapping, agreement on approach and nomenclature is targeted first step
- Proficiency ratings and scale definition are really important
- Refining these components can add tremendous value to KSATs outlined in *NIST Special Publication 800-181*
- 800-181 is government centric and could be well served by consideration of levels found in government i.e. Security Analyst I, II, III, IV
  - Proficiency and competency for job roles could be very different depending on level and experience of SMEs involved

Pitfalls of Misstating Proficiency

- Failure to adequately define (and agree upon) proficiency scale will adversely affect mapping
  - Proficiency and difficulty ‘compression’
- An example from exam development – scientific passing point study results highlight the need for SME calibration and context
- Uncalibrated results could tend towards an inflated ‘rush to the top’

Examples from Known JTA Processes

- An augmented approach could involve tasks being grouped for best job fit as baseline or variable
- This would be similar to the exam development job task analysis (JTA) process
- Common JTA process not only identifies required job role knowledge, skills, abilities and tasks, but also how relevant each item is to the job role
- We typically utilize an ICF (importance, criticality, frequency) approach
- This ICF component is often a second step to refine results from brainstorming / general feedback sessions

Calibration Survey as a Next Step

- **One main goal is to define a mapping methodology that yields repeatable and validated results**
- Relevant to training, certification and higher education degree programs
- Broad industry input aids consensus
  - Industry nuances, vertical market sectors, geographic constraints, and regulatory concerns
- 3rd party verification and validation of basic methodology and results is beneficial to all
  - Similar concept to originally envisioned NICCS portal course feedback

Pitfalls of Uncalibrated Coverage and Difficulty

- Normalizing coverage metrics of certification topics to KSATs as precursor to group success
- Mapping many topics to 90+% coverage seems unlikely in the real world
- This can have a duplicative effect when ‘word search’ coverage levels are combined with high proficiency scales
- Its hard to deliver repeatable mapping results without a defined and agreed upon process

Core Capabilities are Important

- Tasks could be grouped for best job fit as baseline (needs) or variable (wants)
- By focusing on correct proficiency and normalized mapping to prioritized baseline KSATs the result could be more meaningful (albeit less complete)
- By focusing on core competencies mapping results could also more repeatable
  - may also drive levels such as beginner, intermediate, advanced

Million Points of Mapping (ouch)

- Sometimes mapping to too many KSATs can also lead to mismatches
  - Going down to the molecular level can get us looking at trees vs. the forest
- KSATs included in current Special Pub 800-181, NICE Cybersecurity Workforce Framework are analogous to initial brain storming of ‘what to not leave out’
- Possible next step of ICF ranking for job role KSATs by industry SMEs could yield a more tangible lexicon

A Few Examples

- Here are a few examples of tasks which would rate high vs. low with an ICF scale
- baseline / common to job success - Needs
- variable / less common to job success - Wants

Example 1:

Cyber Defense Analyst - PR-CDA-001 (ISACA)

- Task evaluation
  - 29% core vs. 68% variable
  - 1 outlier
- Skills evaluation
  - 43% core vs. 57% variable
- Task rating higher on ICF scale (baseline / common to job success)
  - T0259 Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.
- Task rating lower on ICF scale (variable / less common to job success)
  - T0298 Reconstruct a malicious attack or activity based off network traffic.

Example 2:
Systems Security Analyst – OM-ANA-001 (GIAC)

- Three examples of highest ICF Tasks for Systems Security Analyst
  - T0309 Assess the effectiveness of security controls.
  - T0470 Analyze and report system security posture trends.
  - T0499 Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.
- Three examples of lowest ICF Tasks for Systems Security Analyst
  - T0017 Apply service oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.
    - Note: this seems more aligned to role of software design vs. systems security analyst.
  - T0344 Assess all the configuration management (change configuration/release management) processes.
    - note: hard to imagine organizations where the systems security analyst oversees change control or has expertise in assessing such a process
  - T0477 Ensure the execution of disaster recovery and continuity of operations.
    - Note: in practice this seems the job of a business leader. A security analyst typically does not marshal the resources to make this happen.

Conclusion

- Main goal is to define a mapping methodology that yields repeatable and validated results
- Survey of Industry SMEs regarding input on sample job role KSATs via ICF rankings is a possible next step
- Questions?

Q & A

NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

Thank You for Joining Us!

Upcoming Webinar: "**Cybersecurity Careers for Autistic People**"

When: Wednesday, October 18, 2017 at 2:00pm EST

Register: **https://nist-nice.adobeconnect.com/webinar-oct2017/event/registration.html**

nist.gov/nice/webinars