

Agenda

- Moderator
 - Bill Newhouse, NIST
- Panelists
 - Paul Wang, CSU (session proposal submitter)
 - Dan Stein, DHS
 - Corrinne Sande, Whatcom Community College
- Presentation [30 min total]
 - DB development/deployment progress
 - Application domain(s): web, course design/development, others
 - Collaborative effort
 - Contribution to the NICE workforce development framework
- Next steps
- Q&A [15 min]

Building NICE Database for Government, Industry, and Academia

Moderator:

Bill Newhouse, NIST

Panelists:

Paul Wang*, Endowed Chair, CSU

Dan Stein, DHS

Corrinne Sande, Whatcom Community College

History (Bill)

- Nice database group started Nov. 2017
 - Paul Wang created NICE database for an NSA grant
 - Corrinne Sande was planning to create a NICE framework database
 - Alan Watkins has helped push DHS to apply a database structure

Current Status

- About 20 members as of Feb, 2018
- Database shared with academia, industry, and government
- Expand database from relational to non-relational database (Amazon DynamoDB)
- CyberWatch West ([nice-workroles](#)), NICCS ([nice-framework](#))
- Use database for cyber curriculum/training development
- Created sister-database - PCI/DSS and shared with companies such as Coco Cola and TSYS.

Mission

- To provide a NICE framework database for
 - Website to generate dynamic content
 - Be able to search by category, work roles, and KSAs
 - Map with CAE and other frameworks
 - Assist in designing cyber curriculum/training
 - Broaden the NICE community

Panel Introduction

- Paul Wang*, Endowed Chair, CSU
- Dan Stein, DHS
- Corrinne Sande, Whatcom Community College

Paul Wang

- Build NICE framework DB for cyber curriculum development
 - Received an NSA grant
 - Development a MS in cyber management program.
 - Developed a number of cyber courses
- Migrated the NICE DB to Amazon DynamoDB (non-relational)
- Presented at NICE, NCS, and CISSE conferences
- Shared the database with academia, industry, and government

NICE Databases - CSU

CCT441W-A.NICE_DB - dbo.Category × SQLQuery1.sql - C...ng_shuangbao (54)

ID	Name	Code	Description
1	Securely Provision	SP	Specialty areas concerned with conceptualizing, designing, and b...
2	Operate and Maintain	OM	Specialty areas responsible for providing the support, administrati...
3	Oversee and Govern	OV	Oversight and Development - Specialty areas providing leadershi...
4	Protect and Defend	PR	Specialty areas responsible for the identification, analysis, and mit...
5	Analyze	AN	Specialty areas responsible for highly specialized review and evalu...
6	Collect and Operate	CO	Specialty areas responsible for specialized denial and deception o...
7	Investigate	IN	Specialty areas responsible for the investigation of cyber events a...
* NULL	NULL	NULL	NULL

994	Securely Pro...	Risk Manage...	Secur
995	Securely Pro...	Risk Manage...	Secur
996	Securely Pro...	Risk Manage...	Secur
997	Securely Pro...	Risk Manage...	Secur
998	Securely Pro...	Risk Manage...	Secur
999	Securely Pro...	Risk Manage...	Secur
1...	Securely Pro...	Risk Manage...	Secur

Query executed successfully.

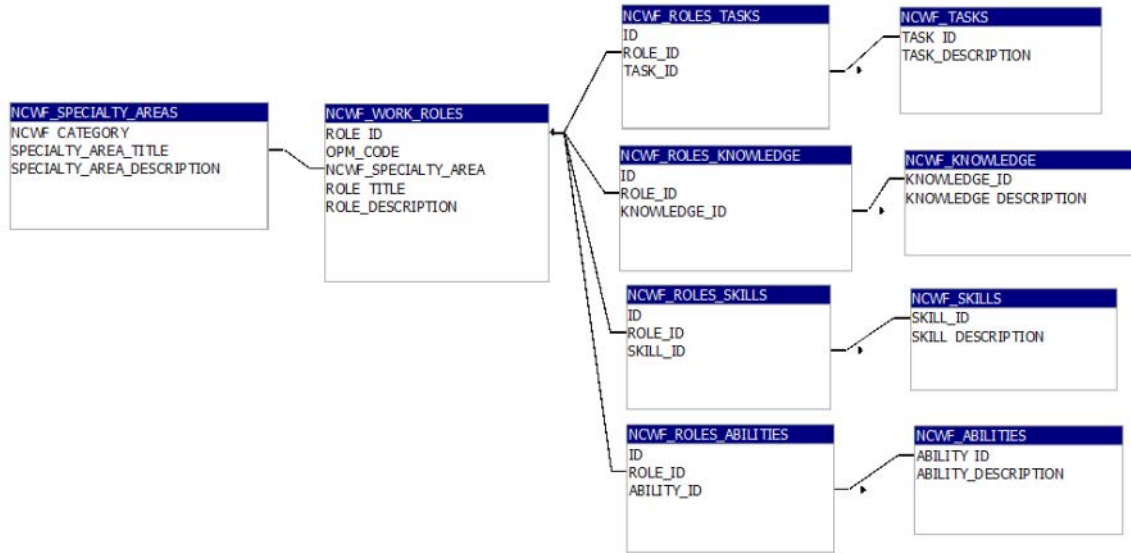
ID	Ca...	Name	Code	Description
1	1	Risk Management	RSK	Oversees, evaluates, and supp
2	1	Software Development	DEV	Develops and writes/codes ne
3	1	Systems Architecture	ARC	Develops system concepts an
4	1	Technology R&D (TRD)	TRD	Conducts technology assessm
5	1	Systems Requirements Planning	SRP	Consults with customers to g
6	1	Test and Evaluation	TST	Develops and conducts tests
7	1	Systems Development	SYS	Works on the development pl

ID	S...	Name	Code	Definition
1	1	Authorizing Official/Des...	SP-RSK-001	Senior official or executive with
2	1	Security Control Assessor	SP-RSK-002	Conducts independent compre
3	2	Software Developer	SP-DEV-001	Develops, creates, maintains, ar
4	2	Secure Software Assessor	SP-DEV-002	Analyzes the security of new or
5	3	Enterprise Architect	SP-ARC-001	Develops and maintains busine
6	3	Security Architect	SP-ARC-002	Ensures that the stakeholder se
7	4	Research & Developme...	SP-TRD-001	Conducts software and system:

NICE framework database for NSA cybersecurity curriculum development grant (Paul)

NICE Databases -

Relationships for NCWF_Roles_v01
Friday, September 8, 2017



NCWF Single Ability Report
Listing of all Work Roles associated selected Ability

Selected Ability: Ability ID (Display only) | Ability description (Display only)

WORK ROLES:

Work Role ID (Display only)	Work Role Title (Display only)
Work Role Description 1 (Display only)	

NCWF Category: NCWF Category-1 (Display only) | Specialty Area: Specialty Area-1 (Display only)

Work Role ID-2 (Display only)	Work Role Title-2 (Display only)
Work Role Description-2 (Display only)	

NCWF Category: NCWF Category-2 (Display only) | Specialty Area: Specialty Area-2 (Display only)

NOTE: If lines of Work Role information will continue until all related work roles are displayed.

Defined many queries with mock-up pages (Alan)

NICE Database - NICCS

Categories/Specialty Areas | Work Roles | Tasks | Skills | Knowledge | Abilities | Keyword Search



Analyze

Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Specialty Areas ▾



Collect and Operate

Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

Specialty Areas ▾



Investigate

Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Specialty Areas ▾



Operate and Maintain

Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

Specialty Areas ▾



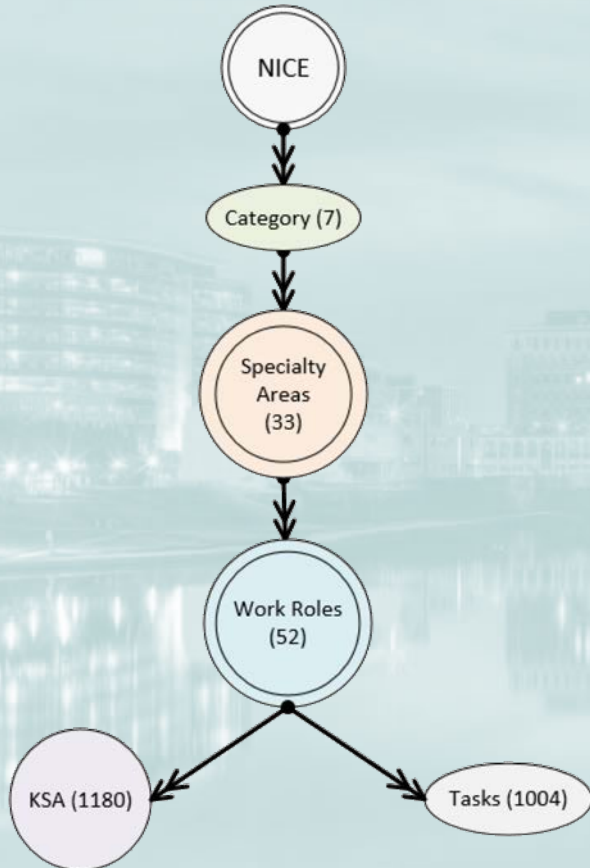
Oversee and Govern

Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.

Specialty Areas ▾

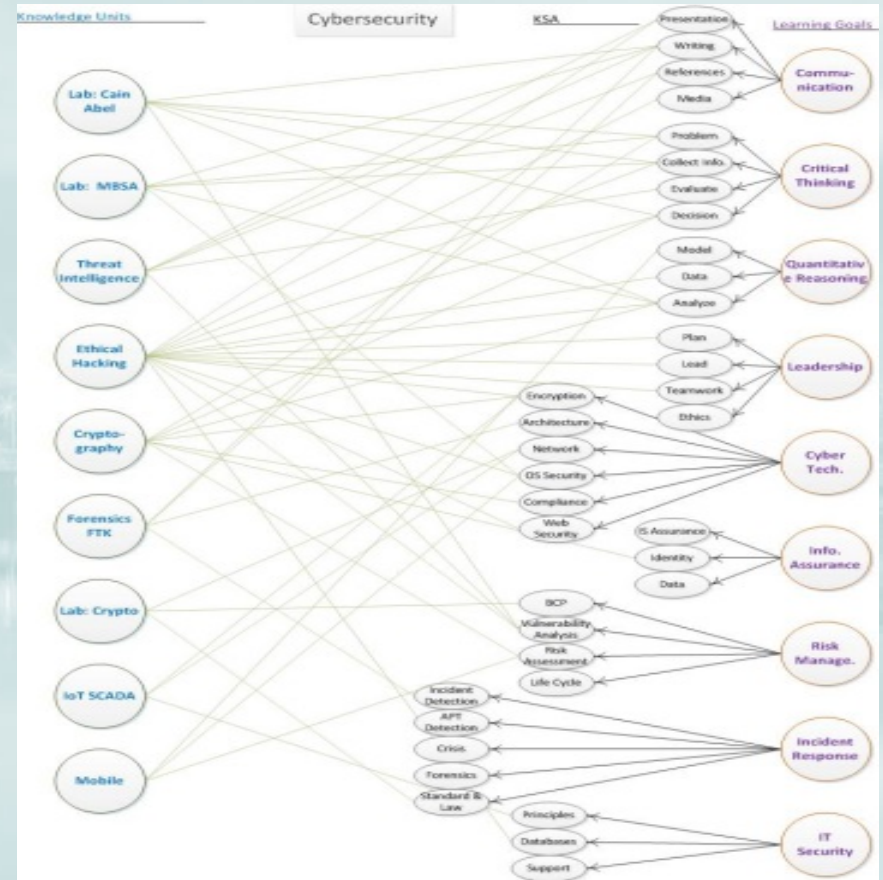
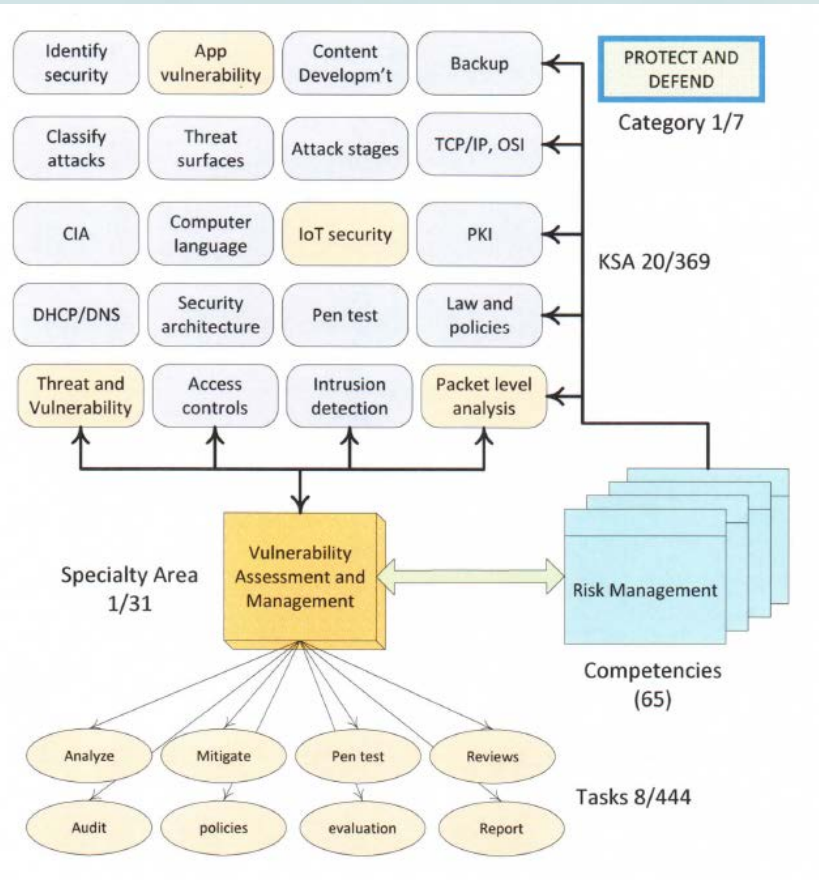
DHS website to allow search tasks and KSAs

Framework and Mapping

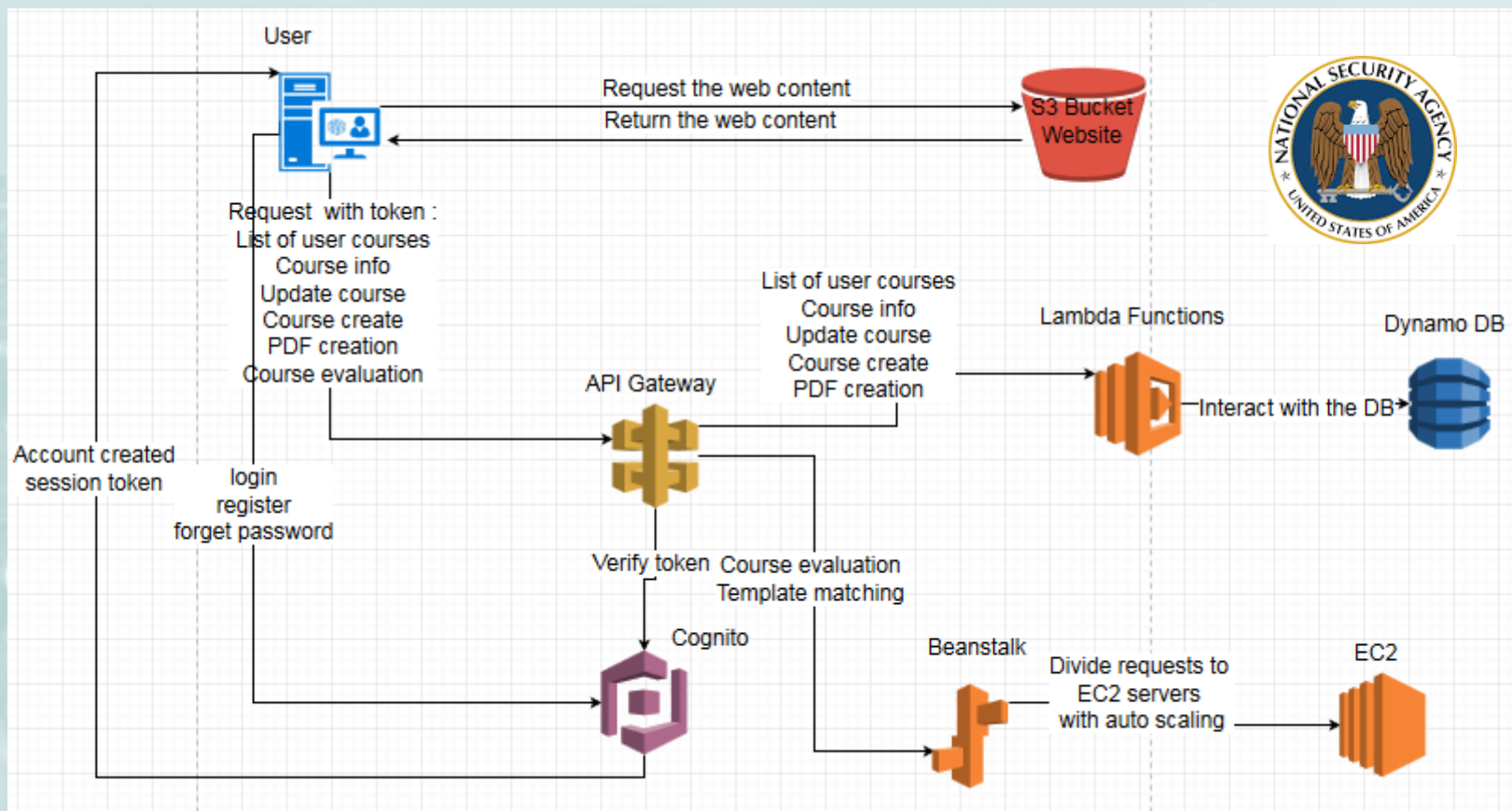


Goal/Competency/Description	Learning Demonstrations									
	1	2	3	4	5	6	7	8	9	10
5.1 Encryption: Knowledge of procedures, tools, and applications used to keep data or information secure, including public key infrastructure, point-to-point encryption, and smart cards.	Yellow			Yellow	Yellow	Yellow				
5.2 Enterprise Architecture: Knowledge of architectural methodologies used in the design and development of information systems, including the physical structure of a system's internal operations and interactions with other systems and knowledge of standards that either are compliant				Yellow					Yellow	Yellow
5.3 Computer Network Defense : Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats				Yellow			Yellow		Yellow	Yellow
5.4 Operating System Security: Identify potential threats to operating systems and the security features necessary to guard against them.		Yellow		Yellow				Yellow		

User NICE DB for Cyber Course Design

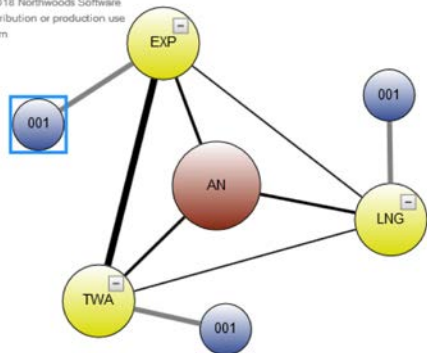


AWS Architecture

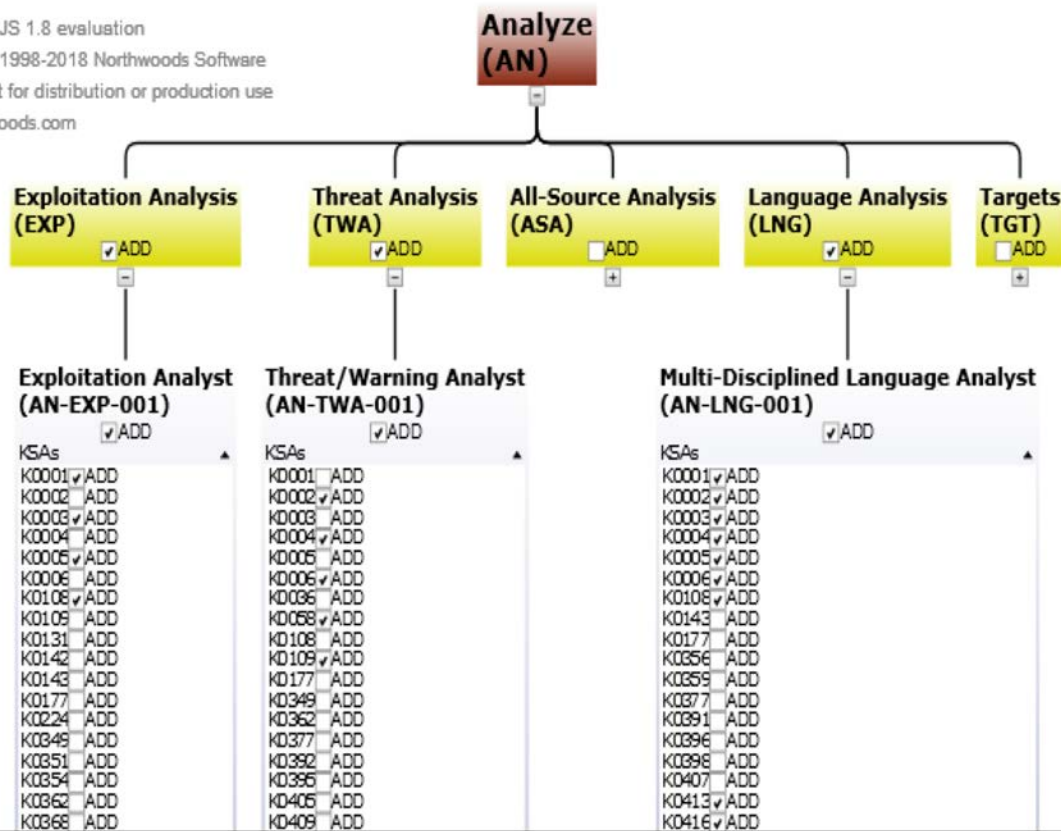


Curriculum/Training Design

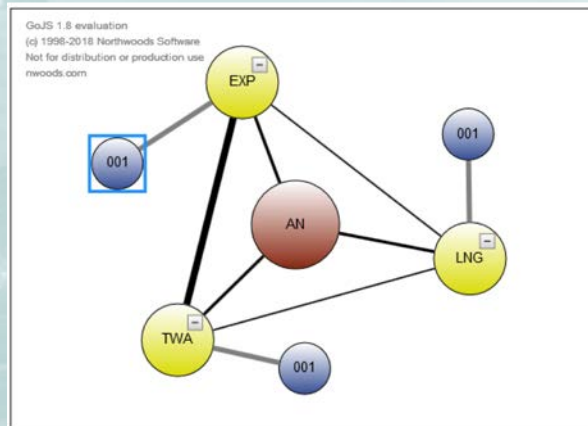
GoJS 1.8 evaluation
 (c) 1998-2018 Northwoods Software
 Not for distribution or production use
 nwoods.com



GoJS 1.8 evaluation
 (c) 1998-2018 Northwoods Software
 Not for distribution or production use
 nwoods.com



Curriculum/Training Design



GoJS 1.8 evaluation
(c) 1998-2018 Northwoods Software
Not for distribution or production use
nwoods.com

Analyze (AN)

- Exploitation Analysis (EXP)** ADD
 - Exploitation Analyst (AN-EXP-001)** ADD
 - KSAs
 - K0001 ADD
 - K0002 ADD
 - K0003 ADD
 - K0004 ADD
 - K0005 ADD
 - K0006 ADD
 - K0108 ADD
 - K0109 ADD
 - K0131 ADD
 - K0142 ADD
 - K0143 ADD
 - K0177 ADD
 - K0224 ADD
 - K0349 ADD
 - K0351 ADD
 - K0354 ADD
 - K0362 ADD
 - K0368 ADD
- Threat Analysis (TWA)** ADD
 - Threat/Warning Analyst (AN-TWA-001)** ADD
 - KSAs
 - K0001 ADD
 - K0002 ADD
 - K0003 ADD
 - K0004 ADD
 - K0005 ADD
 - K0006 ADD
 - K0036 ADD
 - K0058 ADD
 - K0108 ADD
 - K0109 ADD
 - K0177 ADD
 - K0349 ADD
 - K0362 ADD
 - K0377 ADD
 - K0392 ADD
 - K0396 ADD
 - K0405 ADD
 - K0409 ADD
- All-Source Analysis (ASA)** ADD
- Language Analysis (LNG)** ADD
 - Multi-Disciplined Language Analyst (AN-LNG-001)** ADD
 - KSAs
 - K0001 ADD
 - K0002 ADD
 - K0003 ADD
 - K0004 ADD
 - K0005 ADD
 - K0006 ADD
 - K0108 ADD
 - K0143 ADD
 - K0177 ADD
 - K0356 ADD
 - K0359 ADD
 - K0377 ADD
 - K0391 ADD
 - K0396 ADD
 - K0398 ADD
 - K0407 ADD
 - K0413 ADD
 - K0416 ADD
- Targets (TGT)** ADD



viCyber project website

<https://vicyber.columbusstate.edu/>

NICE framework database

paul.wang@computer.org

DAN STEIN, DHS

<https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework>

CORRINNE SANDE

<http://cyberindustry.org/workrole>



Next Step

- Mobile DB
- NoSQL DB
- New models and views
- Applications
 - Workforce development
 - Mappings with other frameworks
 - AI and knowledge base

Q&A

