NICE Framework Alignment Matrix

Competency Mapping for Curriculum Approval

Overview

This document provides a detailed mapping between our Human-AI Partnership activities and the NICE Framework (NIST SP 800-181 Rev 1, Version 2.0.0) Task, Knowledge, and Skill (TKS) statements. These alignments support curriculum approval processes for K-12 cybersecurity education programs and demonstrate how classroom activities develop authentic workforce competencies.

For Curriculum Administrators

This matrix demonstrates standards alignment for state/district cybersecurity curriculum approval. All TKS codes reference the official NICE Framework available at niccs.cisa.gov.

TKS Cross-Reference Matrix

This matrix shows at a glance which NICE Framework competencies each activity addresses. Use the search and filter features (HTML) or scan the checkmarks to quickly identify coverage patterns.

How to Read This Matrix

- ✓ **(Checkmark)**: Activity addresses this competency
- – **(Dash)**: Activity does not specifically address this competency
- **Grouped by**: Tasks (T), Knowledge (K), and Skills (S)

Coverage Summary

Quick Reference: Activity-to-Work-Role Mapping

Activity	Primary Focus	Related Work Roles	Key Competency Areas
Security Detective Teams	Threat detection & analysis	Cyber Defense Analyst, Vulnerability Assessment Analyst	Log analysis, pattern recognition, anomaly identification
Ethics in Automated Security	Policy & governance	Cyber Policy Planner, Privacy Officer	Policy development, stakeholder analysis, risk assessment
AI-Assisted Incident Response	Incident handling	Incident Responder, Cyber Defense Analyst	Incident coordination, response procedures, communication

Activity 1: Security Detective Teams

Competency Alignment

Students practice foundational skills aligned with **Cyber Defense Analysis** and **Vulnerability Assessment** work areas.

Tasks Practiced

Code	Task Statement	Activity Connection
T1084	Identify anomalous network activity	Students analyze system logs to identify unusual patterns that may indicate security incidents
T1118	Identify vulnerabilities	Students discover weaknesses in security practices (e.g., password reuse patterns)
T1119	Recommend vulnerability remediation strategies	Students propose solutions after identifying security gaps

Knowledge Developed

Code	Knowledge Statement	Activity Connection
K0682	Knowledge of cybersecurity threats	Students learn to recognize indicators of potential threats in log data
K0683	Knowledge of cybersecurity vulnerabilities	Students identify common vulnerability patterns (credential exposure, access anomalies)
K0684	Knowledge of cybersecurity threat characteristics	Students distinguish between normal and suspicious activity patterns
K0751	Knowledge of system threats	Students understand how attackers exploit system weaknesses
K0752	Knowledge of system vulnerabilities	Students recognize technical and human factors that create vulnerabilities

Skills Practiced

Code	Skill Statement	Activity Connection
S0540	Skill in identifying network threats	Students determine which anomalies represent genuine security concerns
S0544	Skill in recognizing vulnerabilities	Core activity: students identify security weaknesses in evidence documents
S0800	Skill in analyzing organizational patterns and relationships	Students correlate data across multiple sources to build complete picture
S0874	Skill in performing network traffic analysis	Students analyze access logs and activity patterns

Activity 2: Ethics in Automated Security

Competency Alignment

Students practice foundational skills aligned with **Cybersecurity Policy** and **Privacy** work areas.

Tasks Practiced

Code	Task Statement	Activity Connection
T1307	Develop cybersecurity policy recommendations	Students create policies balancing security with privacy/fairness
T1308	Coordinate cybersecurity policy review and approval processes	Students consider multiple stakeholder perspectives in policy design
T1605	Advise management, staff, and users on cybersecurity policy	Students present and defend policy recommendations

Knowledge Developed

Code	Knowledge Statement	Activity Connection
K0659	Knowledge of information privacy technologies	Students learn how AI systems handle personal data
K0682	Knowledge of cybersecurity threats	Students understand threats that automated systems address
K0683	Knowledge of cybersecurity vulnerabilities	Students recognize how policies can create or prevent vulnerabilities
K0736	Knowledge of information technology (IT) security principles and practices	Students apply security principles to policy decisions

Skills Practiced

Code	Skill Statement	Activity Connection
S0800	Skill in analyzing organizational patterns and relationships	Students consider how policies affect different stakeholder groups
S0850	Skill in performing cost/benefit analysis	Students evaluate trade-offs in automated security decisions
S0878	Skill in performing risk analysis	Students weigh security benefits against privacy/fairness risks

Activity 3: AI-Assisted Incident Response

Competency Alignment

Students practice foundational skills aligned with **Incident Response** and **Cyber Defense** work areas.

Tasks Practiced

Code	Task Statement	Activity Connection
T1221	Disseminate incident and other Computer Network Defense (CND) information	Students coordinate information sharing across team roles
T1300	Report cybersecurity incidents	Students document and communicate incident findings
T1310	Implement protective or corrective measures when a cybersecurity incident or vulnerability is discovered	Students make decisions about containment and remediation

Knowledge Developed

Code	Knowledge Statement	Activity Connection
K0682	Knowledge of cybersecurity threats	Students identify threat actors and attack vectors
K0684	Knowledge of cybersecurity threat characteristics	Students understand attacker tactics, techniques, and procedures
K0724	Knowledge of incident response principles and practices	Students learn structured approach to incident handling
K0725	Knowledge of incident response tools and techniques	Students use AI as an incident response tool
K0726	Knowledge of incident handling tools and techniques	Students apply containment and eradication concepts

Skills Practiced

Code	Skill Statement	Activity Connection
S0540	Skill in identifying network threats	Students determine scope and nature of security incidents
S0800	Skill in analyzing organizational patterns and relationships	Students coordinate team response across multiple roles
S0878	Skill in performing risk analysis	Students assess incident severity and business impact

Grade-Band Progression

Each activity introduces NICE Framework competencies at developmentally appropriate levels, building complexity as students advance through grade bands:

Grade Band	Competency Focus	Cognitive Level	Activity Adaptation
K-2	Awareness	Recognition	Identify ”helpers” vs. ”bad actors” in simple scenarios
3-5	Understanding	Comprehension	Explain why patterns matter and what makes activity suspicious
6-8	Application	Analysis	Analyze evidence with AI partnership, correlate multiple data sources
9-12	Evaluation	Synthesis	Critique AI recommendations, design policies, lead incident response

Cross-Cutting Competencies

All three activities develop these foundational competencies:

Human-AI Collaboration Skills

Competency	NICE Alignment	Development Across Activities
Critical evaluation of AI outputs	S0544, S0800	All activities require students to verify AI findings
Complementary task allocation	T1084, T1118, T1310	Students learn which tasks benefit from AI vs. human analysis
Contextual judgment	K0682, K0684	Students provide context that AI systems cannot access

Professional Communication

Competency	NICE Alignment	Development Across Activities
Technical documentation	T1300, T1221	Students document findings and decisions
Stakeholder communication	T1605, T1308	Students present findings to different audiences
Team coordination	T1310, T1221	Students work in roles with distinct responsibilities

Using This Matrix

For Curriculum Approval

When preparing curriculum approval documentation, reference specific TKS codes to demonstrate standards alignment. Map activity learning objectives to corresponding NICE competencies, and document how grade-band progressions build systematically toward workforce readiness.

For Assessment Design

Use TKS statements to create competency-based rubric criteria that align assessment evidence with specific skill demonstrations. This approach enables educators to track student progression across competency areas over time.

For Career Pathway Planning

Connect classroom activities to authentic workforce competencies by introducing students to cybersecurity career language. These connections build awareness of diverse cybersecurity roles and help students envision potential career pathways.

References

- NIST Special Publication 800-181 Revision 1: Workforce Framework for Cybersecurity (NICE Framework)
- NICE Framework Version 2.1.0 (December 2025)
- Available at: https://niccs.cisa.gov/workforce-development/nice-framework

Category	Code	Competency	Detective	Ethics	AI Response
Tasks	T1084	Identify anomalous network activity	✓	—	✓
Tasks	T1118	Identify vulnerabilities	✓	—	—
Tasks	T1119	Recommend vulnerability remediation strategies	✓	—	—
Tasks	T1221	Disseminate incident and CND information	—	—	✓
Tasks	T1300	Report cybersecurity incidents	—	—	✓
Tasks	T1307	Develop cybersecurity policy recommendations	—	✓	—
Tasks	T1308	Coordinate cybersecurity policy review processes	—	✓	—
Tasks	T1310	Implement protective/corrective measures	—	—	✓
Tasks	T1605	Advise on cybersecurity policy	—	✓	—
Knowledge	K0659	Information privacy technologies	—	✓	—
Knowledge	K0682	Cybersecurity threats	✓	✓	✓
Knowledge	K0683	Cybersecurity vulnerabilities	✓	✓	—
Knowledge	K0684	Cybersecurity threat characteristics	✓	—	✓
Knowledge	K0724	Incident response principles and practices	—	—	✓
Knowledge	K0725	Incident response tools and techniques	—	—	✓
Knowledge	K0726	Incident handling tools and techniques	—	—	✓
Knowledge	K0736	IT security principles and practices	—	✓	—
Knowledge	K0751	System threats	✓	—	—
Knowledge	K0752	System vulnerabilities	✓	—	—
Skills	S0540	Identifying network threats	✓	—	✓
Skills	S0544	Recognizing vulnerabilities	✓	—	—
Skills	S0800	Analyzing organizational patterns and relationships	✓	✓	✓
Skills	S0850	Performing cost/benefit analysis	—	✓	—
Skills	S0874	Performing network traffic analysis	✓	—	—
Skills	S0878	Performing risk analysis	—	✓	✓

Category	Total Codes	Activity 1	Activity 2	Activity 3
Knowledge	10	5	4	5
Skills	6	4	3	3
Tasks	9	3	3	4
Total	25	12	10	12