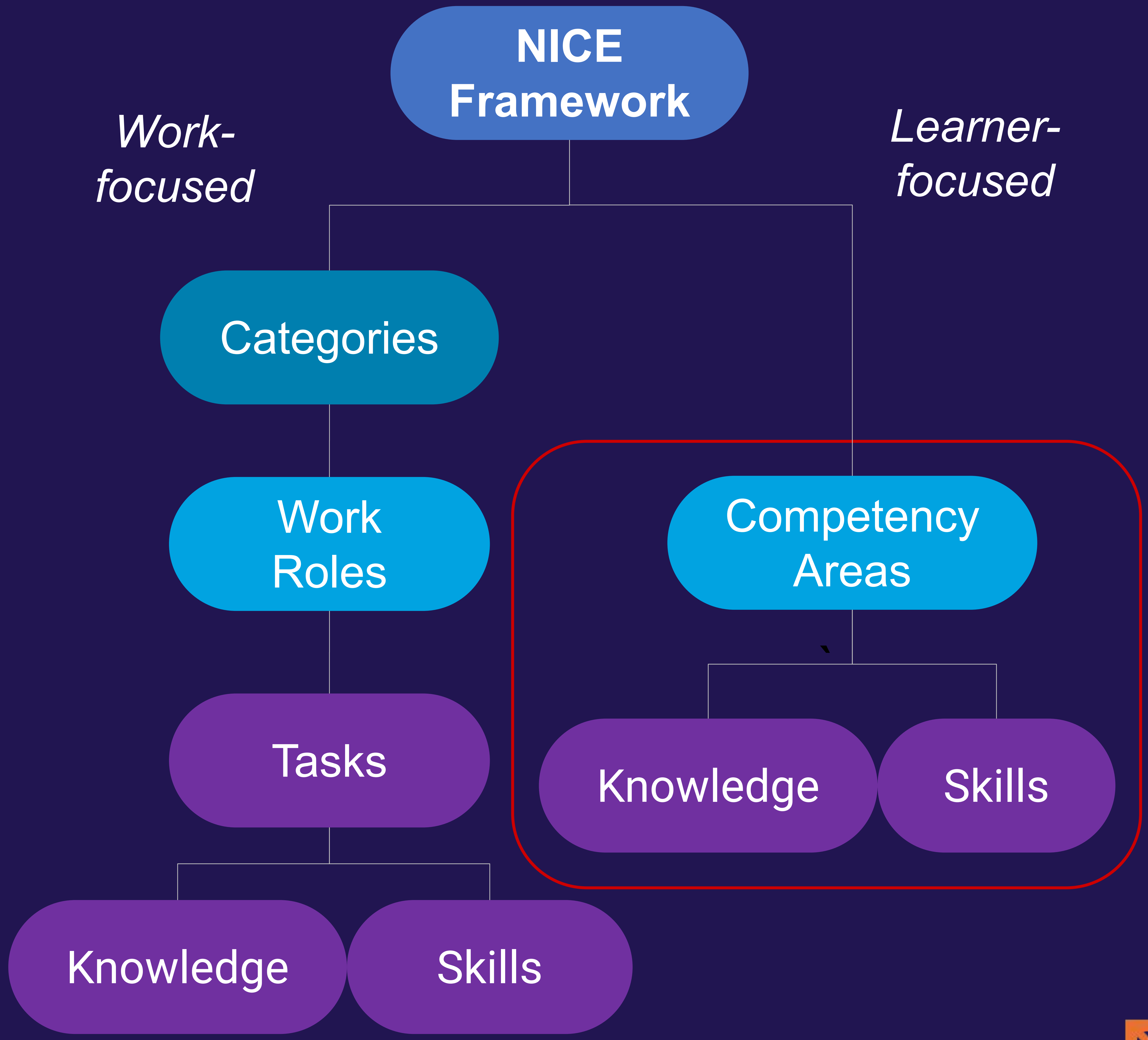
Incorporating AI Tasks, Knowledge, and Skills in the NICE Framework

The NICE Framework provides a common language for describing cybersecurity work. New content informed by NIST publications and subject matter experts will provide practitioners in government, industry, and academia with actionable workforce standards related to **1)** *cybersecurity risks in AI development and implementation* and **2)** *the use of AI systems across areas of cybersecurity work.*



1) Cybersecurity of AI systems: Competency Area development
With support from MITRE—and reference to NIST publications such as the AI RMF and other federal initiatives led by NSF, NSA, and DoD—NICE is developing a new AI Security Competency Area slated for release for public comment in late 2024/early 2025.

>>> *Competency Areas* are clusters of Knowledge and Skill statements correlated with capability in a domain like AI Security. They can be applied across Work Roles (e.g., Systems Testing, R&D, or Privacy Compliance).

2) AI for cybersecurity: New Tasks, Knowledge, Skill statements
On an ongoing basis, NICE will develop additional Task, Knowledge, and Skill statements to reflect uses of AI technology across cybersecurity functions (e.g., threat modeling, malware analysis, report generation).

Share your perspective! Our team needs your input to fully reflect NIST's AI work in the NICE Framework. Contact the NICE Framework team at **NICEframework@nist.gov** to share ideas or schedule a meeting.

AI@NIST Day, September 19, 2024
Presented by Mike Prebil, Cybersecurity Workforce Analyst