

Developing a Workforce to Secure Operational Technologies

A NICE Framework Workshop

Tuesday, August 24, 2021
1-5 p.m. ET (10 a.m. - 2 p.m. PT)



CAE in Cybersecurity Community Virtual Event
<https://www.caecommunity.org>

Today's Agenda



- Opening and Welcome
- Operational Technology and the Cybersecurity Workforce
- Industrial Control System Cybersecurity Specific Job Roles
- NICE Framework: Competencies & Work Roles
- Break-out Session: Identifying What is Unique in OT
- *Break*
- Integrating OT into the NICE Framework: Coming to Consensus
- Integrating OT into the NICE Framework: Building the Content
- Closing Session: Where We Go From Here

Today's Goals

Understand **how OT translates to the workforce** and why it's important to cybersecurity.

Discuss sample OT scenarios to determine what is **unique about OT** and what **already is represented** in the NICE Framework.

Understand NICE Framework **Work Roles and Competencies** to determine the best approach to incorporating OT.

Identify **OT tasks** for inclusion in the NICE Framework.

Housekeeping & Ground Rules

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

- Slides will be shared following the event
 - Recording of main sessions for internal review only
 - Mute when not speaking
 - A workshop report will follow
-

- Be present
 - Share *and* listen
 - Keep an open mind
 - Watch out for rabbit holes
-

Opening & Welcome

Rodney Petersen
Director, National Initiative for
Cybersecurity Education (NICE)

NICE
NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



New NICE Strategic Plan Mission

To energize, promote, and coordinate a robust community working together to advance an integrated ecosystem of cybersecurity education, training, and workforce development

New NICE Strategic Plan Goals



Why Include OT in the NICE Framework? And Why Now?

- **May 2019** – America’s Cybersecurity Workforce Executive Order
 - Identify skills, education, and training needed for securing critical infrastructure, in particular cyber-physical systems and control systems
- **November 2019** – Began Review and Updates to NICE Framework
- **December 2019** – Cross Sector Control Systems Working Group (CISA -> NSC)
 - Workforce Development Subgroup (CISA and NICE)
- **January 2020** – Feedback to NICE Framework Request for Comments: Less IT, More OT
- **November 2020** – Revision to NICE Framework Published (NIST SP 800-181)
- **April 2021** – Pre-draft Call for Comments for NIST Guide to Industrial Control Systems (NIST SP 800-82)
- **July 2021** – National Security Memo on Improving Cybersecurity for Critical Infrastructure Control Systems

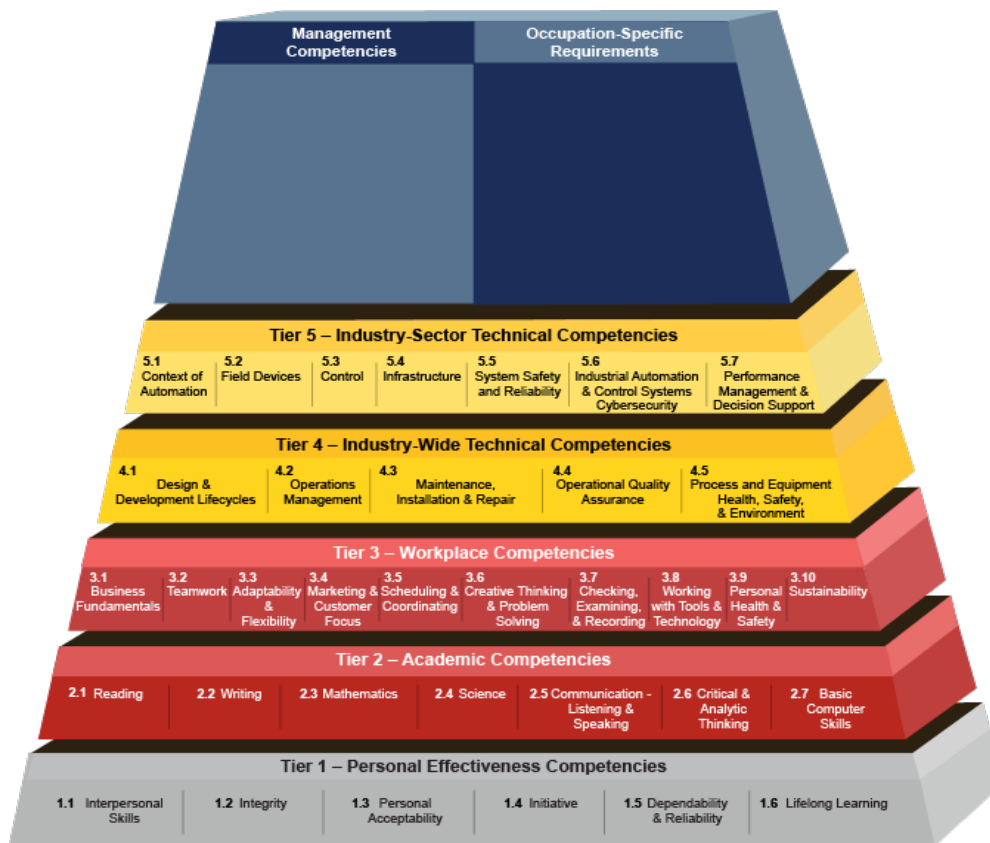


NICE Webinar Series

**Cybersecurity Education and Training for the
Operational Technology Workforce (June 2018)
Securing Operational Technologies and Control Systems
with a Skilled Workforce (July 2021)**

<https://www.nist.gov/itl/applied-cybersecurity/nice/events/webinars>

Automation Competency Model Framework (July 2018)



Source: <https://www.careeronestop.org/competencymodel/competency-models/automation.aspx>

Operational Technology defined

Operational technology (OT) encompasses a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events.

Examples include industrial control systems, building management systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.

Source: NIST OT security landing page

<https://csrc.nist.gov/projects/operational-technology-security>

Industrial Control System Cybersecurity Specific Job Roles

Dean Parsons
ICS Cyber Security Officer, SANS

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION





Industrial Control System Cybersecurity Specific Job Roles

DEAN PARSONS B.Sc. GICSP, GRID, GCIA, GSLC, CISSP

Certified SANS Instructor | Critical Infrastructure Defender | ICS Cyber Security Officer

AUGUST 2021

Introduction



Assessments CISSP Defense Distribution
Electric Ethical Gas GICIA Generation
GRID GSLC Hacking Hunting ICS
Instructor NERC-CIP Officer Oil OT Power
Safety Security Threat Transmission

Converged technologies, resources, built/maintain ICS Security teams - 10 yrs

Established, deployed ICS Security Program across Electric, O & G sectors

Built teams for IT/OT Incident Response, ICS Threat Hunting, ICS Assessments

Manager of Incident Response, Electric Oil & Gas sectors

DEAN PARSONS B.Sc. GICSP, GRID, GICIA, GSLC, CISSP

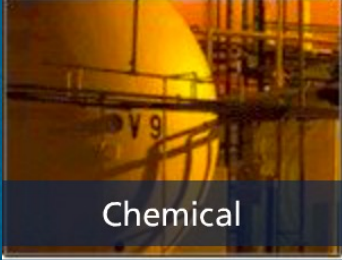
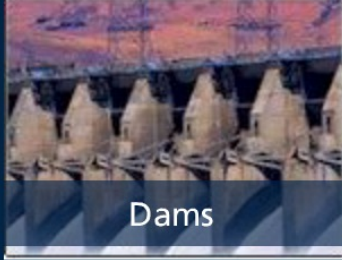




Certified SANS ICS Instructor | Critical Infrastructure Defender | ICS Cyber Security Officer

OUR GOAL TODAY



- ① IT Security & ICS Security Differences
- ② Finding & Retaining ICS Security Skills
- ③ ICS Security Job Roles Walkthrough
- ④ Q & A

ICS Sectors

| | | | |
|---|--|---|--|
|  <p>Chemical</p> |  <p>Dams</p> |  <p>Financial Services</p> |  <p>Commercial Facilities</p> |
|  <p>Defense Industrial Base</p> |  <p>Food and Agriculture</p> |  <p>Communications</p> |  <p>Emergency Services</p> |
|  <p>Government Facilities</p> |  <p>Critical Manufacturing</p> |  <p>Energy</p> |  <p>Healthcare and Public Health</p> |
|  <p>Water Wastewater Systems</p> |  <p>Information Technology</p> |  <p>Nuclear Reactors, Materials, Waste</p> |  <p>Transportation Systems</p> |

IT vs. ICS/OT Incident Impacts

IT Incident - **Impacts** - ICS Incident



IT INCIDENT

Business applications unavailable

Data corruption

Data loss, brand tarnish

ICS INCIDENT

Loss control of physical process

Manipulation of physical process

Personnel Safety, loss of life

IT vs. ICS/OT Incident Impacts

IT Incident - **Impacts** - ICS Incident



Safety of people and physical industrial assets

MOVING / SECURING DATA

ENABLING, SECURING PHYSICS

IT

Vs.

OT





IT – Data vs. ICS/OT - Physics

MOVING DATA VS. ENABLING PHYSICS

Industrial engineering control system assets are often compared to traditional IT assets.

Traditional IT assets focus on data at rest or data in transit.





IT – Data vs. ICS/OT - Physics

MOVING DATA VS. ENABLING PHYSICS

OT/ICS engineering processes and operating technology environments:

Managing, monitoring and controlling real-time systems for physical input values and controlled output physical actions.

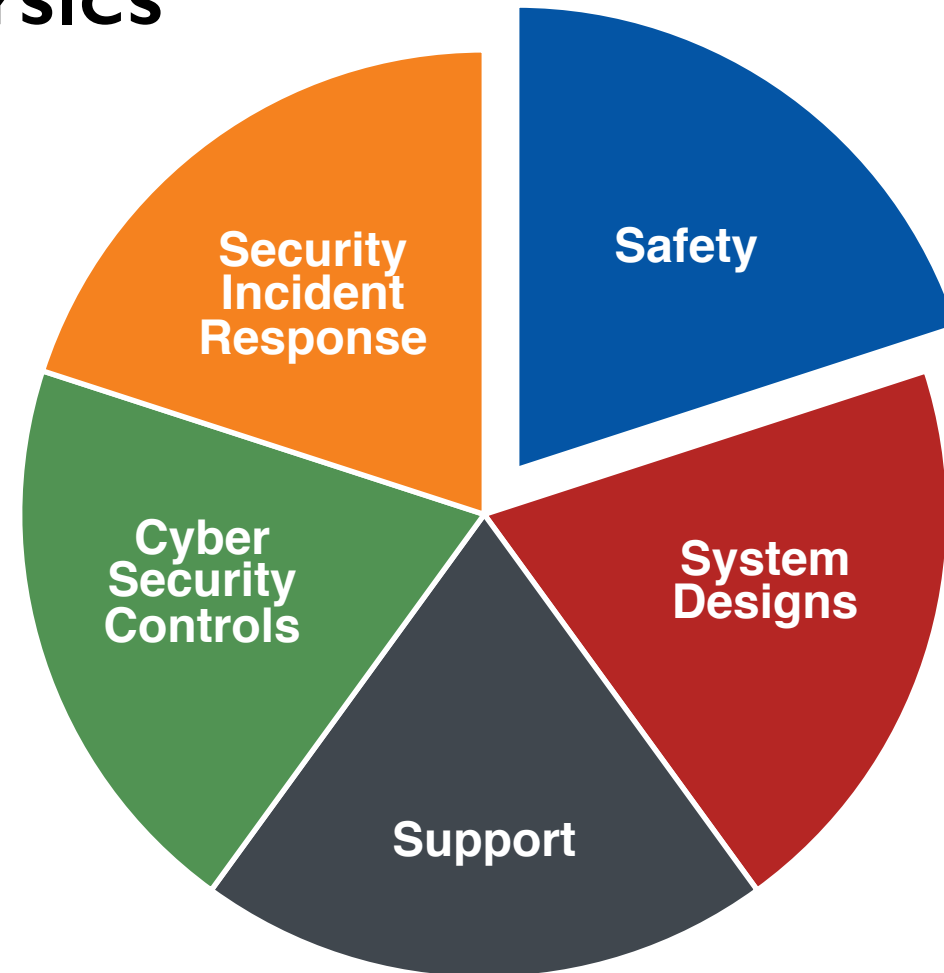




IT – Data vs. ICS/OT - Physics

MOVING DATA VS. ENABLING PHYSICS

It is this primary difference
between IT and OT/ICS
industrial systems that drive
differing:





OT/IT Technology convergence...

It already happened!

*ICS have been utilizing traditional IT **technology** to for industrial purposes in industrial environment for the last 20+ years.*



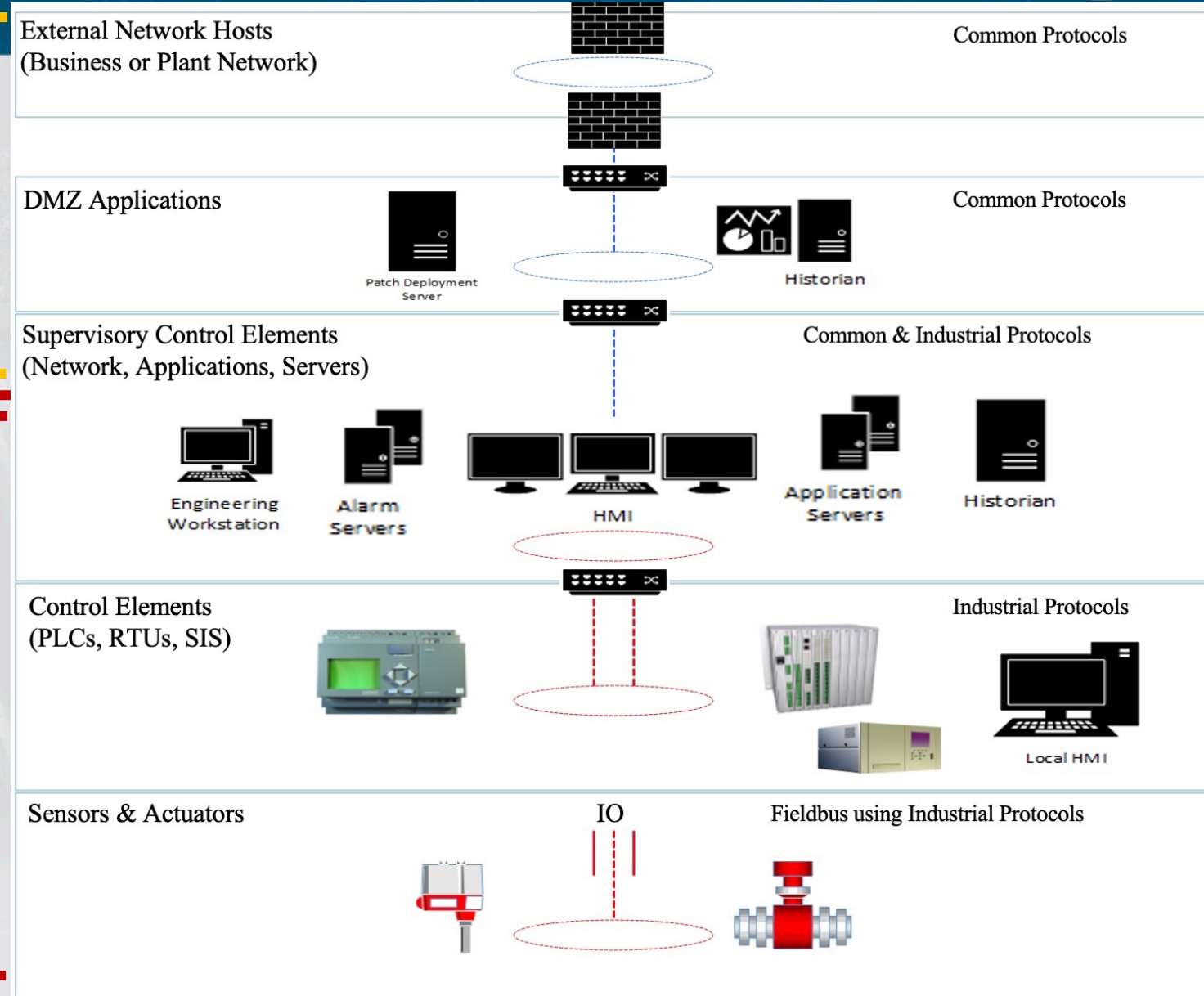
IT – Data vs. ICS/OT - Physics



IT – Data vs. ICS/OT - Physics

IT ←
Common operating systems
Traditional protocols

ICS/OT ←
Operating systems adapted
Industrial protocols
Embedded operating systems
Engineering hardware assets



Traditional IT Incident Response Does not account for:

Safety as #1 priority

Embedded systems

Industrial and proprietary protocols

Real-time engineering systems

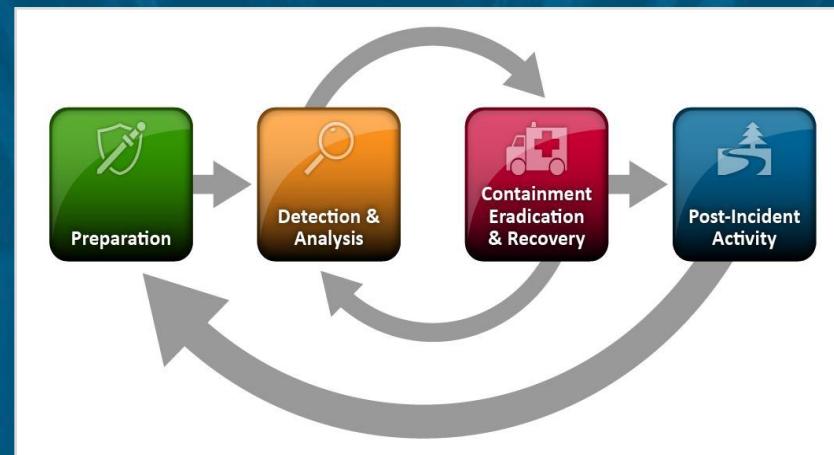
Legacy systems, remote stations, environmental aspects

Preparation

Detection &
Analysis

Containment
Eradication
Recovery

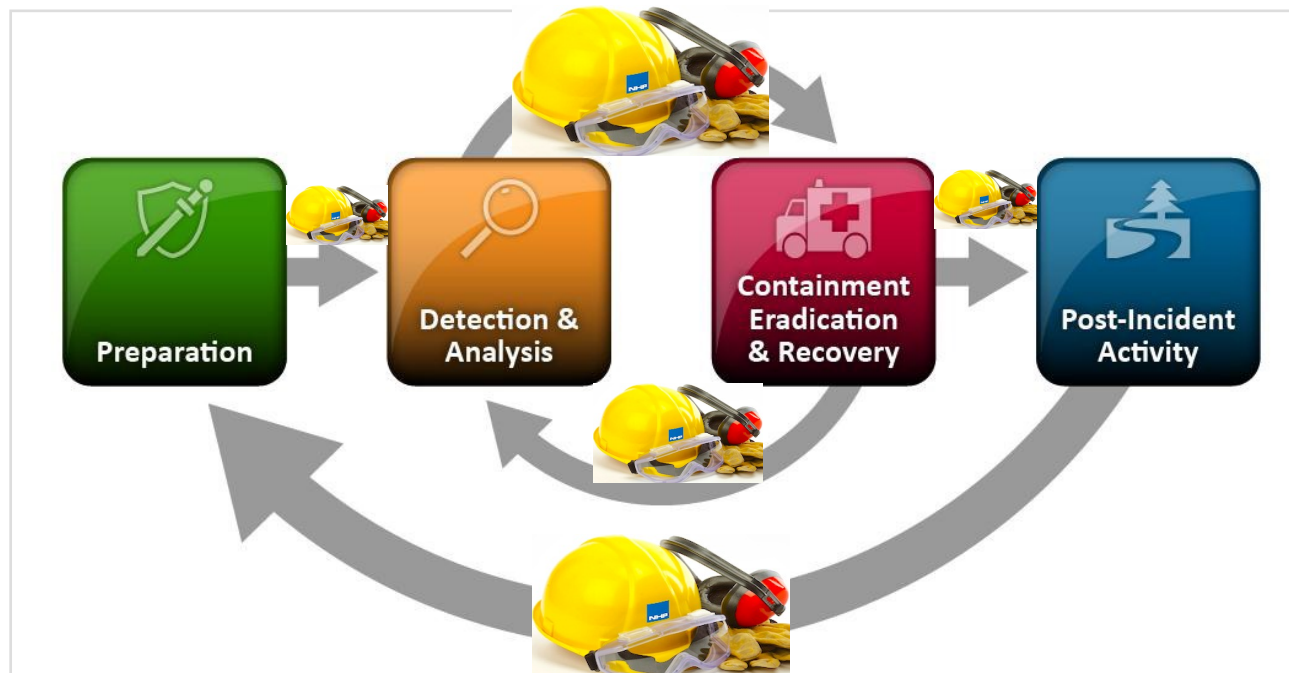
Post Incident
Activity



IT Incident Response \neq ICS Incident Response

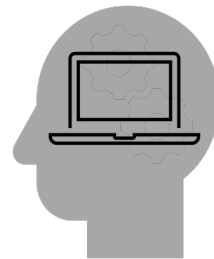


“...incident response deployed in IT business systems may result in ineffective and even disastrous results when applied to ICS cyber incidents.”



OT/IT Team, People convergence...

- A calculator is a tool – used by Finance, HR, Engineering, IT:
- *With different skills, objectives, missions, functions, knowledge of the tool and its' application for a different result.*
- *Does this mean everybody who uses this tool is managed and governed by one manager or the same set of standards and guidance? (split brain)*





OT/IT Team, People convergence...

ICS SECURITY SKILLS: FINDING AND RETAINING ICS TALENT

Hiring from:

IT Security

- Safety – getting them to site
- ICS Security controls, protocols, approach

Process Control, Engineering

- Methods of attacks





IT Incident Response \neq ICS Incident Response

ICS SECURITY SKILLS: FINDING AND RETAINING ICS TALENT

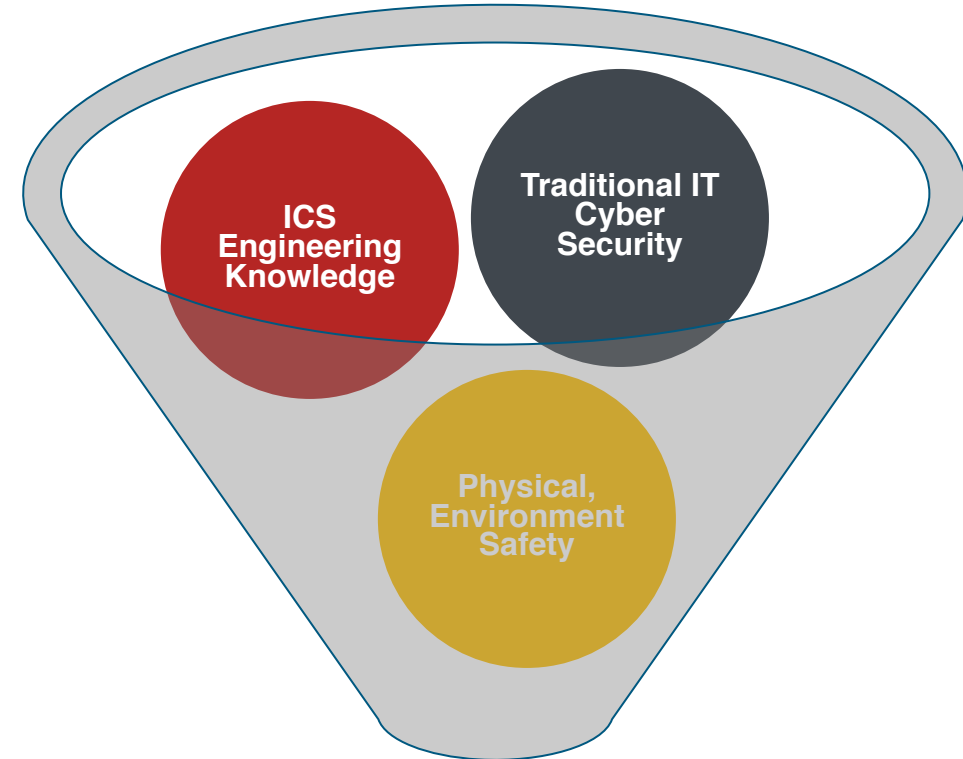
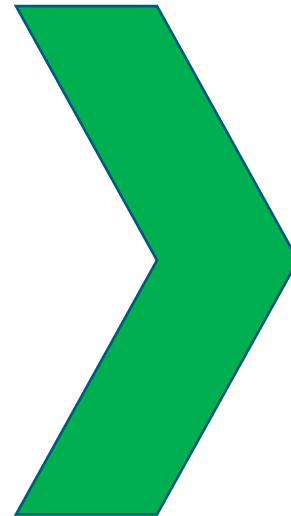
Traditional IT Cyber Security



ICS Engineering Knowledge



Physical, Environmental Safety



ICS Security

ICS Security Specific Roles Needed



OPERATIONS TECHNOLOGY ENGINEERING

Process Control Engineer / Instrument & Control Engineer

- Process control engineers design, test, troubleshoot, and oversee implementation of new processes. In plants with established control systems, the engineers may design and install retrofits to existing systems and troubleshoot hardware, software, and instrument problems in a manner that also preserves the cyber security integrity of ICS.

Security Engineer / ICS Security Analyst/Incident Responder

- Monitor and protect industrial control system environments with the goal of keeping the operational environment **safe, secure, and resilient** against current and emerging cyber threats – both incidental and targeted engineering systems malware or human adversaries.

ICS/OT Systems Engineer

- Designs, builds, and supports engineering and OT systems to support the operations environment and **industrial security design and response**.



OT SECURITY OPERATIONS CENTER

OT Security Operations Manger / ICS Cybersecurity Officer

- A centralized unit from where staff supervises the operations technology and engineering environment with the goal of detecting, analyzing, and responding to cybersecurity incidents, both targeted and now targeted.

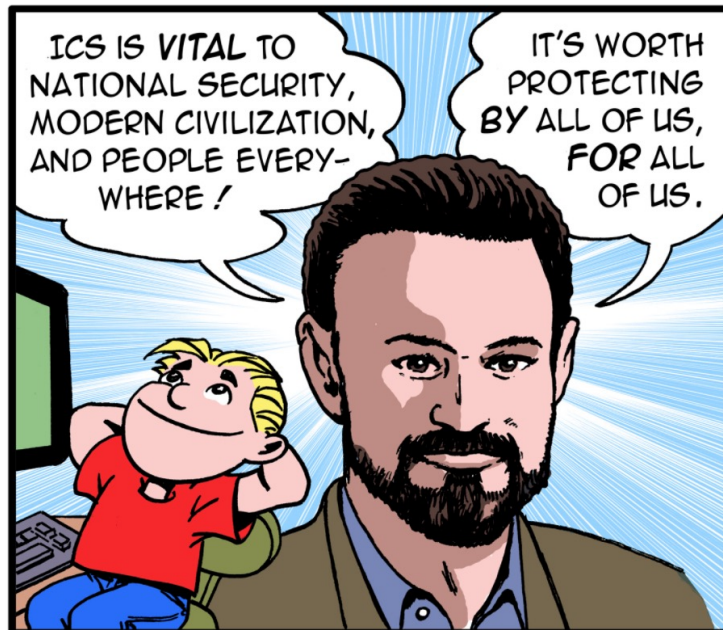
The Mike Assante Principle

“The only defense against well-funded nation-state attacks on power systems (and the rest of the critical infrastructure that keeps us and the economy alive and free) are people with extraordinary cyber [security + safety] talent and skills.”

IT Security \neq ICS Security

- IT Security does not 'paste' into ICS
- ICS DEFENSE IS DOABLE – With trained resources in ICS-aware roles which include skills on safety, engineering equipment, industrial protocols and engineering, networks etc. knowledge.

LITTLE BOBBY



by Robert M. Lee and Jeff Haas

JULY 5TH, 2019-- MIKE HANDED US THE HELM WITH THE WIND AT OUR BACK AND ASKED US TO STAY THE COURSE. WE WILL DO OUR BEST.

THANK YOU! Questions?



DEAN PARSONS B.Sc. GICSP, GRID, GCIA, GSLC, CISSP

Certified SANS Instructor | Critical Infrastructure Defender | ICS Cyber Security Officer



[linkedin.com/in/dean-parsons-cybersecurity](https://www.linkedin.com/in/dean-parsons-cybersecurity)



twitter.com/deancybersec



dparsons@sans.org

NICE Framework: Competencies & Work Roles

Karen Wetzel
Manager of the NICE Framework

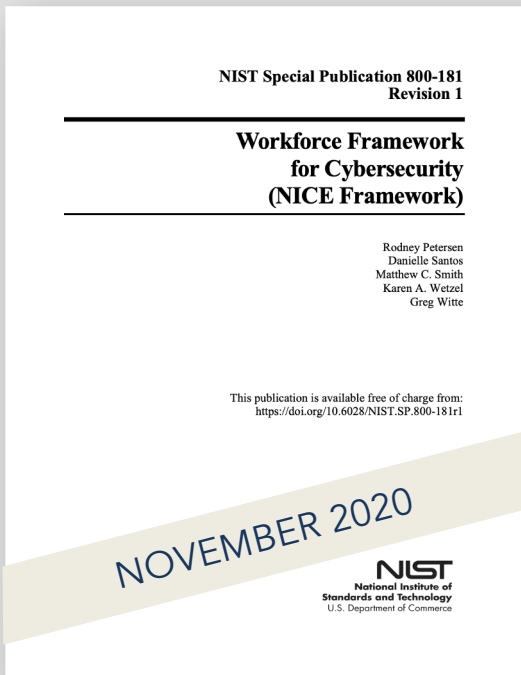
NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



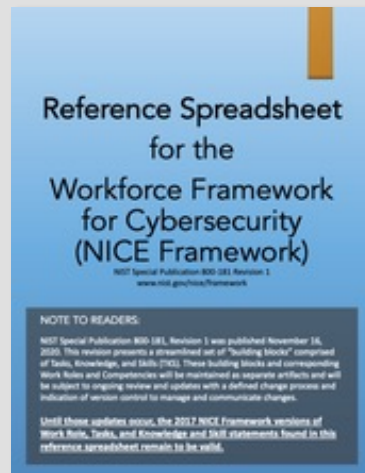
What is it?

Framework Document



[nist.gov/nice/framework](https://www.nist.gov/nice/framework)

Workforce Framework for Cybersecurity (NICE Framework)



Reference Spreadsheet

| Table of Contents | | | | | |
|--|---|---|--------------|------------------------------------|-------------------------------------|
| NICE Specialty Area Description | Work Role | Work Role Description | Work Role ID | KSAs | Tasks |
| Information Systems (IS) - Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development. | | | | | |
| <p>...s, evaluates, and supports the documentation, assessment, and authorization processes to assure that existing and new information technology (IT) systems meet the organization's security and risk requirements. Ensures appropriate treatment of risk, compliance, and security from internal and external perspectives.</p> | Authorizing Official/Designating Representative | 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 (CNSSI 4009). | SP-RSK-001 | Click to view KSAs | Click to view Tasks |
| | Security Control Assessor | Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37). | SP-RSK-002 | Click to view KSAs | Click to view Tasks |
| Software Development (DEV) | Software Developer | Develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs. | SP-DEV-001 | Click to view KSAs | Click to view Tasks |
| | Secure Software Assessor | Analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results. | SP-DEV-002 | Click to view KSAs | Click to view Tasks |
| | Enterprise Architect | Develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures. | SP-ARC-001 | Click to view KSAs | Click to view Tasks |

Table of Contents | [SP-RSK-001 KSAs](#) | [SP-RSK-001 Tasks](#) | [SP-RSK-002 KSAs](#) | [SP-RSK-002 Tasks](#) | [SP-DEV-001 KSAs](#) | [SP-DEV-001 Tasks](#) | [SP-DEV-002 KSAs](#) | [SP-DEV-002 Tasks](#) | +

www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-supplemental-material

Employers

- Track workforce capabilities
- Position descriptions
- Assess learner capabilities
- Develop teams

Education & Training Providers

- Develop a learning program
- Align teaching with NICE Framework
- Assess whether learners have achieved capabilities

Learners

- Learn about a defined area of expertise
- Understand an organization's workforce needs
- Self-assessment

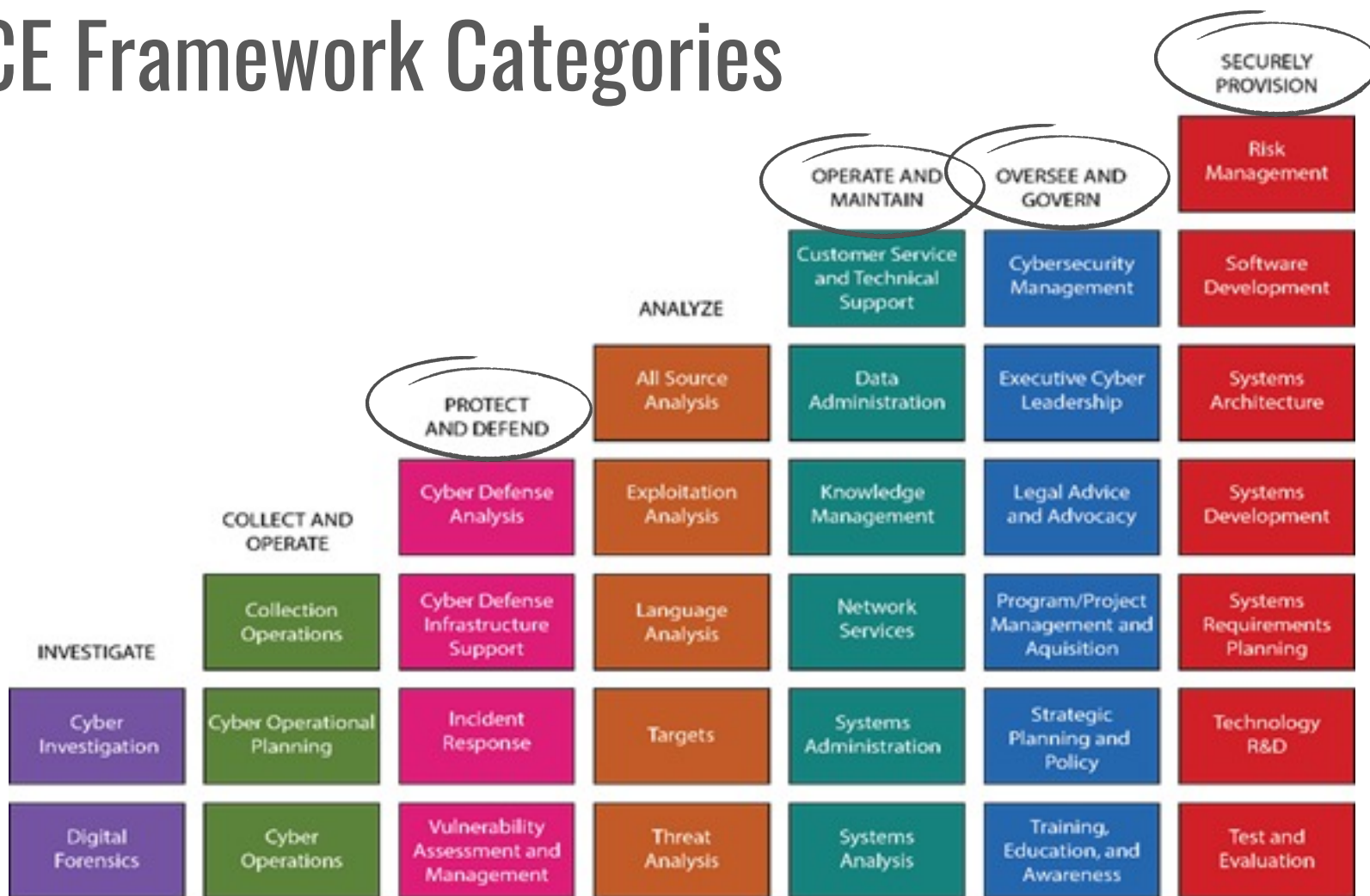
HOW CAN I USE THE
NICE FRAMEWORK?

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

NICE Framework by the Numbers

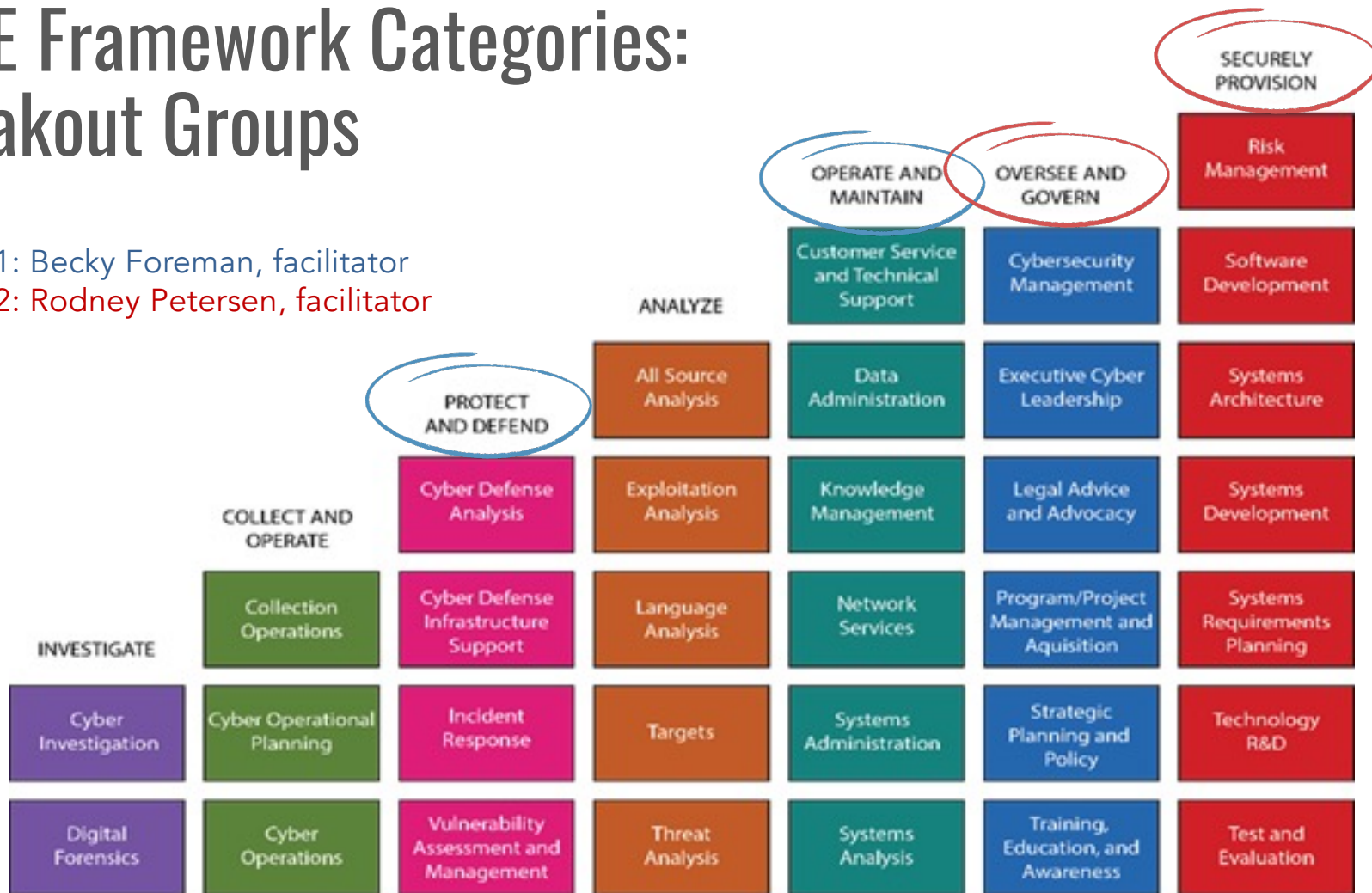


NICE Framework Categories



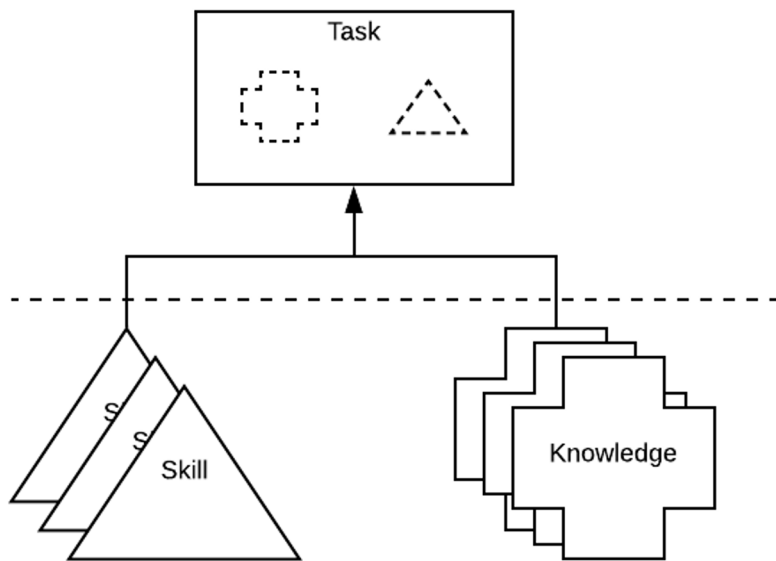
NICE Framework Categories: Breakout Groups

Group 1: Becky Foreman, facilitator
 Group 2: Rodney Petersen, facilitator



NICE Framework Building Blocks

Task, Knowledge, and Skill (TKS) Statements



Using the NICE Framework: Building Block Applications



TEAMS

- Defined by Competencies or Work Roles



COMPETENCIES

- Groupings of TKS
- Means of assessing a learner



WORK ROLES

- Groupings of Tasks
- Work someone is responsible for

Work Roles & Competencies

What do they offer?

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

- A common language to describe cybersecurity work
- A way to identify job and qualification requirements
- Assessment-based hiring and promotion
- A means to identify current gaps and training needs and anticipate future requirements
- A way to align work with organizational objectives
- A way to align education and training to organizational goals
- A flexible approach – can be combined with other Work Roles and Competencies

NICE Framework Work Roles

Work Role:

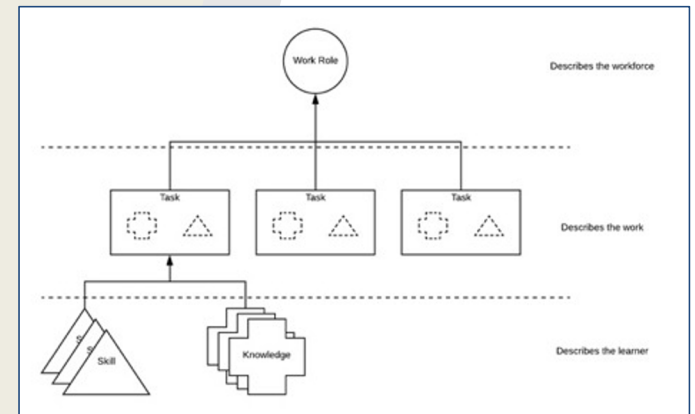
A grouping of work for which someone is responsible or accountable

Work Roles:

- Are not synonymous with job titles or occupations
- May apply to many varying job titles
- Can be combined to create a particular job

Consist of:

- Tasks that constitute the work to be done



Proposed New Work Role: Security Awareness & Engagement Manager

| | |
|-----------------------|--|
| Category | OVERSEE & GOVERN (OV): Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work. |
| Work Role | Security Awareness & Engagement Manager |
| Work Role Description | Builds, maintains, and measures the organization's security awareness and communications program with the goal of securing the workforce's behaviors and ultimately creating a secure culture. |
| Related Competencies | <ul style="list-style-type: none">• Education and Training Delivery• Education and Training Curriculum Development• Professional Competencies (E.g., Communication, Interpersonal Skills)• Organizational Awareness• Risk Management• Law, Policy, and Ethics |

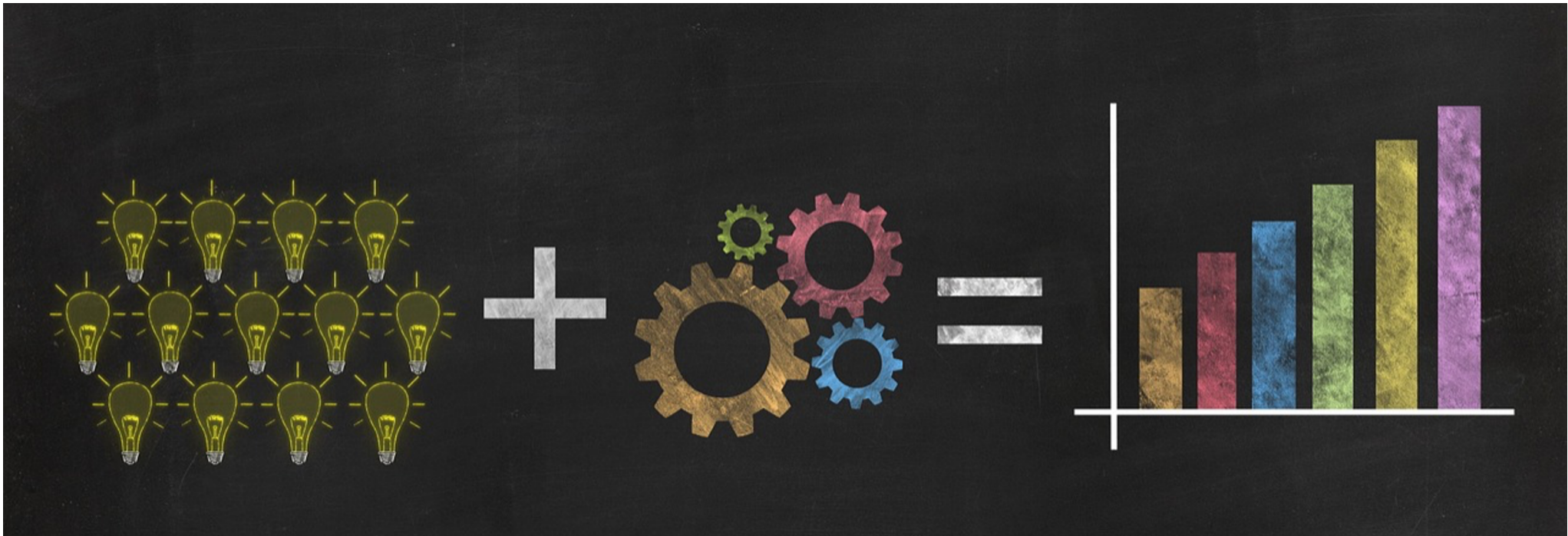
Related TKS

~35 Task Statements

~50 Knowledge and Skill Statements

Some example task statements:

| | |
|-------|---|
| T0001 | Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk. |
| T0157 | Oversee the information security training and awareness program. |
| T0073 | Develop new or identify existing awareness and training materials that are appropriate for intended audiences. |
| T0467 | Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness. |
| T0882 | Conduct on-going privacy training and awareness activities |
| T0206 | Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities. |
| T0248 | Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. |
| T0384 | Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals. |
| T0868 | Work with business teams and senior management to ensure awareness of "best practices" on privacy and data security issues. |



**A clearly articulated, observable framework
for what success looks like.**

"Why Competencies Are the Future of HR" (HR Magazine/SHRM: April 2017)

NICE Framework Competencies

Competency:

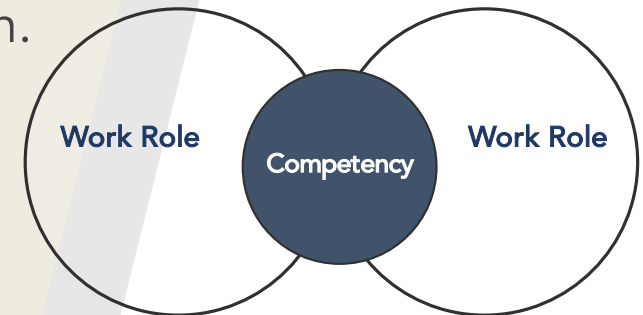
A mechanism for organizations to assess learners (including students, job-seekers, and employees) as well as a means for learners to demonstrate capability in a particular domain.

Competencies are:

- Defined via an employer-driven approach
- Learner-focused
- Can apply to multiple Work Roles, although a Work Role can also stand independent of the Competency

Consist of:

- Competency title
- Competency description
- Associated TKS statements



Draft NISTIR 8355

**NICE Framework Competencies:
Assessing Learners for Cybersecurity Work**

[https://csrc.nist.gov/
publications/detail/nistir/8355/draft](https://csrc.nist.gov/publications/detail/nistir/8355/draft)

NICE Framework Competency Examples

| Competency Title | Competency Type | Competency Description |
|-----------------------------|-----------------|--|
| Contracting and Procurement | Organizational | This Competency describes a learner's capabilities related to procuring, negotiating, administering, and managing various types of contracts, including application of contracting or procurement techniques and requirements according to applicable laws and policies. |
| Infrastructure Design | Technical | This Competency describes a learner's capabilities related to the architecture and topology of software, hardware, and networks, including LANS, WANS, and telecommunications systems, their components and associated protocols and standards, and how they operate and integrate with one another and with associated controlling software. |
| Strategic Planning | Leadership | This Competency describes a learner's capabilities related to formulating effective tactics and metrics associated with the vision, mission, goals, and objectives of the organization or business unit. |
| Communication | Professional | This Competency describes a learner's capabilities related to the process of clearly and effectively expressing information or ideas to individuals or groups in a variety of ways (verbal, nonverbal, written, and visual). Includes understanding when and how to adapt messages for different audiences as well as listening to others' instructions, ideas and intentions, attending nonverbal cues, and responding appropriately. |

How Do They Differ?

Competencies

- Learner focused
- Help address employer needs
- Assessment is typically based on the competency as a whole

Work Roles

- Work focused
- Help define positions and responsibilities
- Assessment typically occurs at the task level

Discussion

- What is driving the need for OT in the NICE Framework?
- What are the biggest challenges for us to address?
- What questions do you have?

Break-out Session: Identifying What is Unique in OT

Becky Foreman, Facilitator

NICE

NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION





Break
Rejoin at 3:15 p.m. ET

12:15 p.m. PT

Integrating OT into the NICE Framework: Coming to Consensus

Becky Foreman, Facilitator

NICE
NATIONAL INITIATIVE FOR **CYBERSECURITY** EDUCATION



Integrating OT into the NICE Framework: Building the Content

Becky Foreman, Facilitator



Closing Session: Where We Go From Here

Karen Wetzel
Manager, NICE Framework

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION



How to Engage

NICE
NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION



Visit the NICE Framework Resource Center
www.NIST.gov/NICE/Framework



Contribute your Success Stories or **Ask** questions
niceframework@nist.gov



Join the [NICE Framework Users Group](#) to
discuss and learn more

Contact me at karen.wetzel@nist.gov



THANK YOU