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

- 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)
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

- NICE Framework
- Learning Process
- Career Discovery
- Talent Management
- Research
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*

Industrial Control System Cybersecurity Specific Job Roles

Dean Parsons
ICS Cyber Security Officer, SANS
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
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, GCIA, 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
<table>
<thead>
<tr>
<th>Chemical</th>
<th>Dams</th>
<th>Financial Services</th>
<th>Commercial Facilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense Industrial Base</td>
<td>Food and Agriculture</td>
<td>Communications</td>
<td>Emergency Services</td>
</tr>
<tr>
<td>Government Facilities</td>
<td>Critical Manufacturing</td>
<td>Energy</td>
<td>Healthcare and Public Health</td>
</tr>
<tr>
<td>Water Wastewater Systems</td>
<td>Information Technology</td>
<td>Nuclear Reactors, Materials, Waste</td>
<td>Transportation Systems</td>
</tr>
</tbody>
</table>
### IT vs. ICS/OT Incident Impacts

<table>
<thead>
<tr>
<th>IT INCIDENT</th>
<th>ICS INCIDENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business applications unavailable</td>
<td>Loss control of physical process</td>
</tr>
<tr>
<td>Data corruption</td>
<td>Manipulation of physical process</td>
</tr>
<tr>
<td>Data loss, brand tarnish</td>
<td>Personnel Safety, loss of life</td>
</tr>
</tbody>
</table>
IT vs. ICS/OT Incident Impacts

IT Incident - Impacts - ICS Incident
Safety of people and physical industrial assets

MOVING / SECURING DATA

IT Vs. OT

ENABLELING, SECURING 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.*
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 is this primary difference between IT and OT/ICS industrial systems that drive differing:
It already happened!

*ICS have been utilizing traditional IT technology to for industrial purposes in industrial environment for the last 20+ years.*
Safety of people and physical industrial assets
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
“...incident response deployed in IT business systems may result in ineffective and even disastrous results when applied to ICS cyber incidents.”
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)
**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
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

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 Manager / 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 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 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.

by Robert M. Lee and Jeff Haas

ICS IS VITAL TO NATIONAL SECURITY, MODERN CIVILIZATION, AND PEOPLE EVERYWHERE!

IT’S WORTH PROTECTING BY ALL OF US, FOR ALL OF US.

ATTACKERS DON’T STAND A CHANCE!

WHO ARE YOU TALKING TO LITTLE BOBBY?

JUST THINKING ABOUT THE REASON WHY DEFENSE WILL WIN IN THE END!
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
twitter.com/deancybersec
dparsons@sans.org
NICE Framework: Competencies & Work Roles

Karen Wetzel
Manager of the NICE Framework
What is it?

Workforce Framework for Cybersecurity (NICE Framework)

Framework Document

Reference Spreadsheet

HOW CAN I USE THE NICE FRAMEWORK?

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
NICE Framework by the Numbers

**Categories**
High-level way to sort Work Roles into related areas. Includes: Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Collect and Operate, and Investigate.

**Work Roles**
A grouping of work for which someone is responsible or accountable. Consist of Tasks that constitute the work to be done.

**Task Statements**
Define the work to be done

**Skill Statements**
Define what someone must be able to do to complete a Task.

**Competencies**
A mechanism for organizations to assess learners. Consist of TKS statements that define the area of work. May be additive to Work Roles.

**Knowledge Statements**
Define what someone must know to complete a Task.
NICE Framework Categories

https://resources.infosecinstitute.com/topic/what-is-the-nice-cybersecurity-workforce-framework/
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?

- 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

<table>
<thead>
<tr>
<th>Category</th>
<th>OVERSEE &amp; GOVERN (OV): Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work Role</td>
<td>Security Awareness &amp; Engagement Manager</td>
</tr>
<tr>
<td>Work Role Description</td>
<td>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.</td>
</tr>
</tbody>
</table>
| Related Competencies | • Education and Training Delivery  
                          • Education and Training Curriculum Development  
                          • Professional Competencies (E.g., Communication, Interpersonal Skills)  
                          • Organizational Awareness  
                          • Risk Management  
                          • Law, Policy, and Ethics |
**Some example task statements:**

<table>
<thead>
<tr>
<th>T0001</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0157</td>
<td>Oversee the information security training and awareness program.</td>
</tr>
<tr>
<td>T0073</td>
<td>Develop new or identify existing awareness and training materials that are appropriate for intended audiences.</td>
</tr>
<tr>
<td>T0467</td>
<td>Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness.</td>
</tr>
<tr>
<td>T0882</td>
<td>Conduct on-going privacy training and awareness activities.</td>
</tr>
<tr>
<td>T0206</td>
<td>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.</td>
</tr>
<tr>
<td>T0248</td>
<td>Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.</td>
</tr>
<tr>
<td>T0384</td>
<td>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.</td>
</tr>
<tr>
<td>T0868</td>
<td>Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues.</td>
</tr>
</tbody>
</table>
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
<table>
<thead>
<tr>
<th>Competency Title</th>
<th>Competency Type</th>
<th>Competency Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contracting and Procurement</td>
<td>Organizational</td>
<td>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.</td>
</tr>
<tr>
<td>Infrastructure Design</td>
<td>Technical</td>
<td>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.</td>
</tr>
<tr>
<td>Strategic Planning</td>
<td>Leadership</td>
<td>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.</td>
</tr>
<tr>
<td>Communication</td>
<td>Professional</td>
<td>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.</td>
</tr>
</tbody>
</table>
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
Rejoin at 3:15 p.m. ET

12:15 p.m. PT
Integrating OT into the NICE Framework: Coming to Consensus

Becky Foreman, Facilitator
Integrating OT into the NICE Framework: Building the Content

Becky Foreman, Facilitator
Closing Session: Where We Go From Here

Karen Wetzel
Manager, NICE Framework
<table>
<thead>
<tr>
<th>How to Engage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Visit</strong> the NICE Framework Resource Center <a href="http://www.NIST.gov/NICE/Framework">www.NIST.gov/NICE/Framework</a></td>
</tr>
<tr>
<td><strong>Contribute</strong> your Success Stories or <strong>Ask</strong> questions <a href="mailto:niceframework@nist.gov">niceframework@nist.gov</a></td>
</tr>
<tr>
<td><strong>Join</strong> the <a href="https://www.nist.gov/nice/users-group">NICE Framework Users Group</a> to discuss and learn more</td>
</tr>
</tbody>
</table>

Contact me at [karen.wetzel@nist.gov](mailto:karen.wetzel@nist.gov)
THANK YOU