CWE-CAPEC ICS/OT Special Interest Group

Wednesday, May 18, 2022

ICS/OT Special Interest Group Participants

1. **Alfinie Bullock,**
2. **Andy Kling,** Schneider Electric
3. **Adam Hahn**
4. **Ahmad Sharafi,**
5. **Alex Rodriguez**, PG&E
6. **Amanda Kraus**
7. **Anton Shipulin**
8. **Armada Sramek**
9. **Barry Greene**, Senki
10. **Bayard Johnson**
11. **Bill Newhouse**
12. **Brandon Carter**,
13. **Ben Deering,** ODNI
14. **Ben Sooter**, EPRI
15. **Bill Aubin,** Nozomi Networks
16. **Bill Newhouse**
17. **Bob Hanson,** LLNL
18. **Bob Heinemann**,
19. **Bob Radvanovsky,**
20. **Bradley Nickens**, GE
21. **Cameron Burden,**
22. **Carl Mccants,** ODNI
23. **Chris Charpentier**, GE
24. **Christopher Havey,** Applied Cybersecurity Engineering
25. **Chris Humphrey**, Boeing
26. **Chris Levendis**,
27. **Craig Barrett,** Kinder Morgan
28. **Curtis Taylor**, CyManII
29. **Curt Wiggins**
30. **Cynthia Hsu,** DOE
31. **Dana Thomas**
32. **Dan Bennett,** NREL
33. **Dan Ehrenreich,** SCCE
34. **Danielle Jablanski**,
35. **Daniel Stachan**
36. **Daryl Haegley**,
37. **Dave Halla**
38. **Dave Keppler**
39. **David Nicol,** UIUC & CyManII
40. **David Simpson**,

ICS/OT Special Interest Group Participants

41. **Deborah Kobza**, IACI
42. **Derek Hart**
43. **Dimple Shah**
44. **Dylan Sundy**
45. **Eric Cosman**
46. **Eric Mitchell**, NSA
47. **Eric Strief,** John Deere
48. **Erik Hrin**
49. **Gananand G Kini**,
50. **Greg Ahira**, GE
51. **Greg Bastien,**
52. **Greg Sanchez**
53. **Hadeli Hadeli,** Hitachi Energy
54. **Harry Perper**, Cyber Architecture and Resiliency
55. **Howard Grimes,** CyManII
56. **Iain Deason,** DHS CISA
57. **Ismael Garcia,** NRC
58. **Jarvis Robinson**
59. **Jason Plant**
60. **Jay Gazlay,** DHS CISA
61. **Jen Walker**, Water ISAC
62. **Jennifer Pedersen**
63. **Jeremy Mckeown**
64. **Jess Smith,** PNNL
65. **Jodi Jensen**
66. **Joe Agres,** West Yost
67. **Joe McCormick**
68. **Joe Weiss**
69. **John Almlof**
70. **John Schneider**
71. **John Parmley**, Zuuliot
72. **John Ransom**
73. **Jon Terrell,** Hitachi Energy
74. **Jon White,** NREL
75. **Jose Jimenez**, Sothis
76. **Jose Perez**, Tenable
77. **Joseph Cummings**, NYPA
78. **Joseph Matthews**
79. **Justin Cain**
80. **Karen Wetzel**
81. **Ken Wang, DOD**
82. **Khalid Ansari**, FM Approvals

ICS/OT Special Interest Group Participants

83. **Kimberly Denbow**,
84. **Krystel Castillo**
85. **Lindsey Cerkovnik,** DHS CISA
86. **Marc Sachs,** Auburn University
87. **Martijn Jansen**, Taqa
88. **Martin Kihiko**,
89. **Martin Scheu**, Switch
90. **Marty Edwards**
91. **Matt Bishop,** UC Davis & CyManII
92. **Marie Stanley Collins,**
93. **Matthew Bohne**
94. **Matthew Knoll**, ArcelorMittal
95. **Megan Samford**
96. **Melissa Vice**, Air Force
97. **Michael Chaney,** CyManII
98. **Michael Hok,** Hitachi Energy
99. **Michael Toecker**
100. **Monika Akbar,** UTEP & CyManII
101. **Nik Urlaub,**
102. **Niyu Ogunniyi**, Corteva
103. **Oystein Brekk-Saunderud,** Norma Cyber
104. **Patrick Dale**
105. **Patrick Obruba**
106. **Patti Escatel,** DHS CISA
107. **Paul Zawada**
108. **Pete Tseronis**
109. **Peter Colombo,**
110. **Peter Jackson**
111. **Philip Huff,** UALR
112. **Piotr Pedziwiatr**, Arcelor Mittal
113. **Ralph Ley**
114. **Raymond Savarda**
115. **Rex Wempen**
116. **Rezaur Rahman**
117. **Rich Piazza**, Information Assurance & Trusted Computing
118. **Robert Garry**, GE Gas Power
119. **Robert Murphy**
120. **Roger Johnson,** Novelis

ICS/OT Special Interest Group Participants

121. **Ronald Atwater**,
122. **Ryan Bays,** PNNL
123. **Shane Stailey**
124. **Shannon Hughes**
125. **Sharin Crane**, Boeing
126. **Sharla Artz**
127. **Sherry Hunyadi**
128. **Steve Battista**,
129. **Steve Chapin**,
130. **Steve Granda,** NREL
131. **Stephanie Saravia**,
132. **Stephen Trachian,** Hitachi Energy
133. **Ted Wittmer**
134. **Thomas Ruoff**, DHS, CISA
135. **Todd Riley, Goodyear**
136. **Tom McGoogan**
137. **Tony Turner**, Fortress
138. **Tracy Briggs,** CyManII
139. **Wayne Austad,** CyManII
140. **Wayne Cantrell**
141. **William Welch**
142. **Yasoda Ramchune,** Chevron

ICS/OT Special Interest Group Leadership and Support

1. **Alec Summers,** MITRE
2. **Andrew Kresses,** Nexight Group
3. **Cheri Caddy,** DOE-CESER
4. **Greg Kerr,** Nexight Group
5. **Greg Shannon,** CyManII
6. **Ginger Wright,** INL
7. **Jeff Hahn,** INL
8. **Jeff Mitchell,** INL
9. **Katie Baker,** Nexight Group
10. **Karsten Daponte,** Nexight Group
11. **Lindsay Kishter,** Nexight Group
12. **Stephen Bolotin,** Nexight Group
13. **Steve Christey,** MITRE
14. **Wendy Leibowitz,** Nexight Group

Agenda

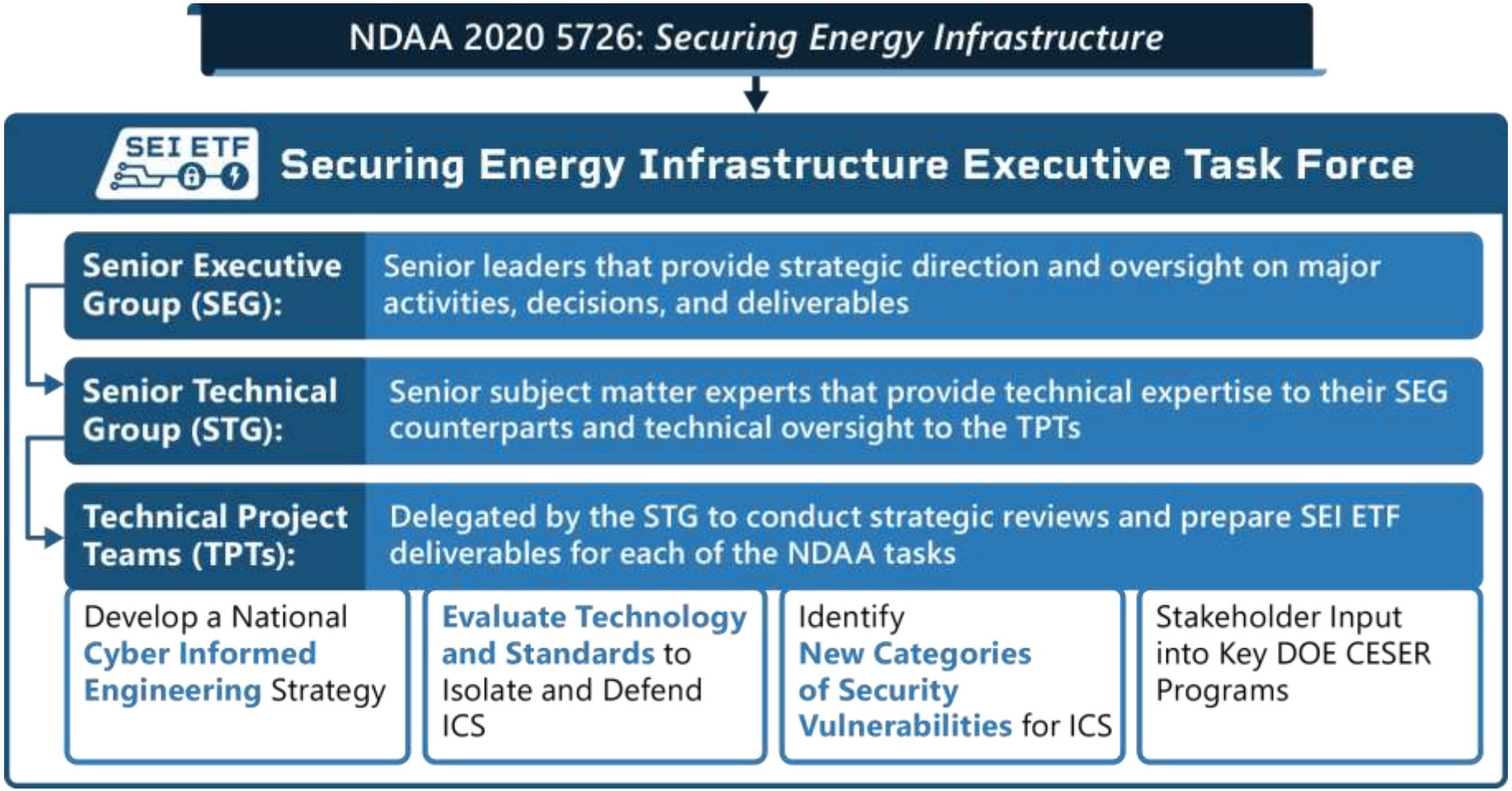
Eastern Time	Activity
3:00 – 3:05 pm	**Login and Roll Call**
3:05 – 3:10 pm	**Opening Remarks** • Greg Shannon, Chief Cybersecurity Scientist, Cybersecurity Manufacturing Innovation Institute (CyManII) • Alec Summers, Principal Cybersecurity Engineer & Group Lead, the MITRE Corporation
3:10 – 3:25 pm	**Introductions and Meeting Purpose** • Introductions from DOE-CESER, MITRE, CyManII, and Nexight Group • High-level overview of ICS/OT Special Interest Group charter • Meeting objectives and outcomes
3:25 – 3:40 pm	**How We Got Here** • Background on the Securing Energy Infrastructure Executive Task Force (SEI ETF) by Cheri Caddy (DOE-CESER) • Background on the Identify New Classes of Security Vulnerabilities (NCSV) Technical Project Team (TPT) by Greg Shannon (CyManII) • Background on Common Weakness Enumeration (CWE) and Common Attack Pattern Enumeration and Classification (CAPEC) by Alec Summers (MITRE)
3:40 – 3:55 pm	**Where We Are Today** • SEI ETF NCSV TPT's 20 categories of security vulnerabilities in ICS/OT systems • Expansion of CAPEC-CWE scope to ICS/OT systems • CWE 4.7 release
3:55 – 4:10 pm	**Related Activities** • CyManII Coordinate Vulnerability Awareness (CVA) • Cyber Informed Engineering (CIE)
4:10 – 4:25 pm	**Where We Want to Go This Year** • Work Plan • Major milestones • SIG meeting cadence
4:30 pm	**Meeting Ends**

Opening Remarks, Introductions & Meeting Purpose

- **Greg Shannon,** Chief Cybersecurity Scientist, Cybersecurity Manufacturing Innovation Institute (CyManII)
- **Alec Summers,** Principal Cybersecurity Engineer & Group Lead, the MITRE Corporation
- **Cheri Caddy,** Senior Advisor, U.S. Department of Energy (DOE), Cybersecurity, Energy Security, and Emergency Response (CESER)
- **Lindsey Cerkovnik,** U.S. Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA)

How We Got Here

BACKGROUND: Securing Energy Infrastructure Executive Task Force (SEI ETF)



BACKGROUND: Identify New Classes of Security Vulnerabilities (NCSV) Technical Project Team (TPT)

KEY DELIVERABLE:

Categories of Security Vulnerabilities in ICS

- Identified **20 Categories of Security Vulnerabilities** that are distinct from those already documented in information technology (IT), go beyond vulnerabilities arising from the implementation of ICS systems, and include those arising from design, architectural, operational, and human factors.
- Now exploring the inclusion of these categories in the Common Weakness Enumeration (CWE) database from the MITRE Corporation.

Examples

1. ICS Communications
   - **Unreliability:** Vulnerabilities arise in reaction to disruptions in the physical layer (e.g., creating electrical noise) used to carry the traffic.
2. ICS Dependencies (& Architecture)
   - **External Physical Systems:** Due to the highly interconnected technologies in use, an external dependency on another physical system could cause an availability interruption for the protected system.
3. ICS Supply Chain
   - **Common Mode Frailties:** At the component level, most ICS systems are assembled from common parts made by other companies. One or more of these common parts might contain a vulnerability that could result in a wide-spread incident.
4. ICS Engineering (Constructions/Deployment)
   - **Maker Breaker Blindness:** Lack of awareness of deliberate attack techniques by people (vs. failure modes from natural causes like weather or metal fatigue) may lead to insufficient security controls being built into ICS systems.
5. ICS Operations (& Maintenance)
   - **Post-Analysis Changes:** Changes made to a previously analyzed and approved ICS environment can introduce new security vulnerabilities (as opposed to safety).

‘Get Ahead of Boom’ Landscape

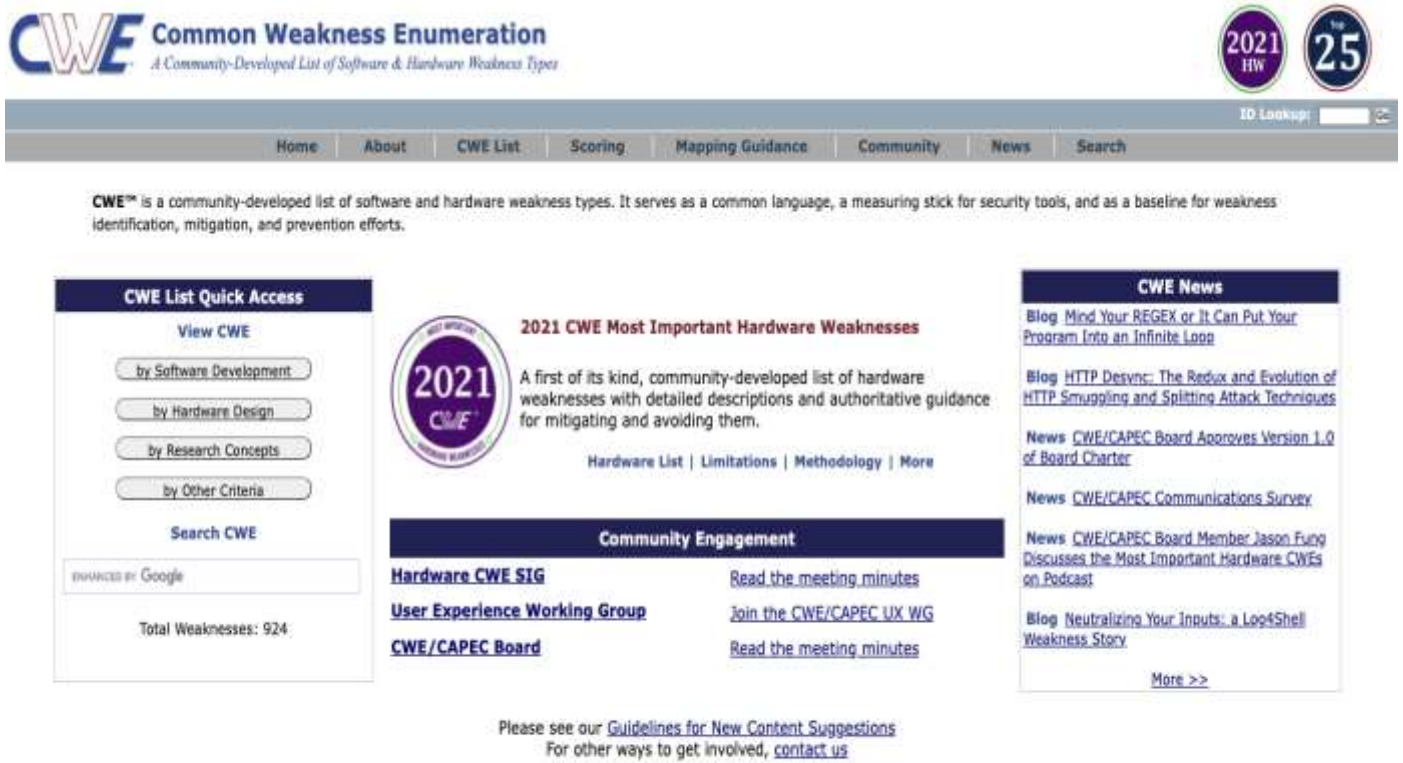
'Get Ahead of Boom' Landscape

CWE is…

CWE™ is a community-developed list of common software and hardware security weaknesses – mistakes that, in proper conditions, could contribute to the introduction of vulnerabilities.

- View all weaknesses related to a category
- Search for a specific weakness type
- Find mapping to other information lists

Vision: CWE informs development, acquisition, and operational efforts resulting in more secure information technology capabilities at lower costs.



CAPEC is…

- **A comprehensive dictionary of attack patterns employed by adversaries to exploit known weaknesses in cyber-enabled capabilities**
- **Built on software 'design patterns'**
  - Paradigms for solving common software design issues
- **'Attack patterns' are 'design patterns' for cyber attackers aimed at exploiting a weakness (CWE)**

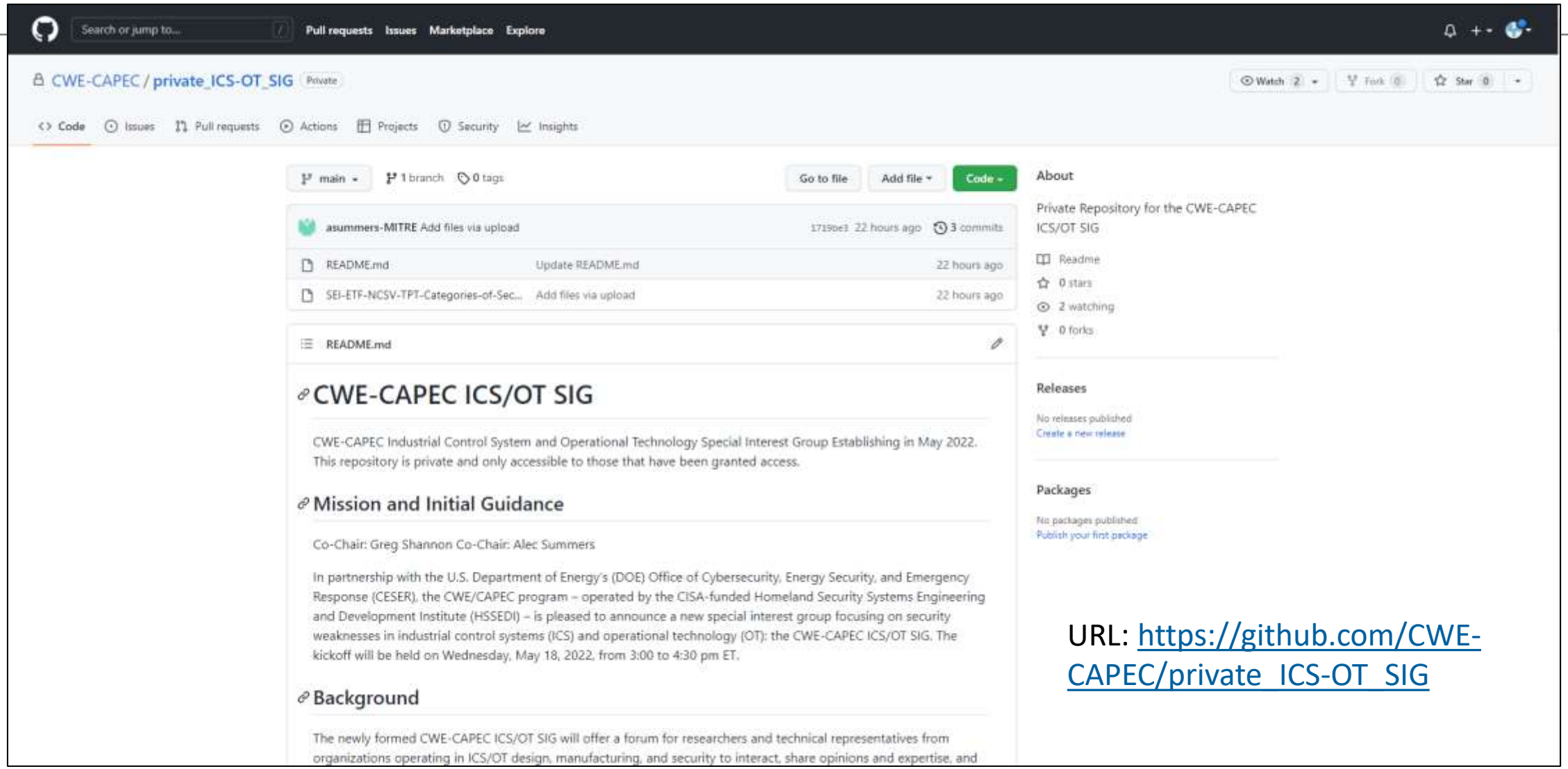
Helping Improve Security Pre-Compromise

CWE/CAPEC Helps Organizations "Shift Left"

- **Enables better security earlier in the development lifecycle by enumerating the weaknesses and related attack patterns to avoid**
  - System designers/developers can be informed about risk from the beginning
  - Product security teams can focus on the weaknesses that they produce
- **Helps make tools easier to use by creating a common language across all tools (e.g., static analysis, dynamic analysis)**
- **Helps users better understand different types of mistakes by providing detailed information about individual weakness types**

Where We Are Today

20 Categories of Security Vulnerabilities



URL: https://github.com/CWE-CAPEC/private_ICS-OT_SIG

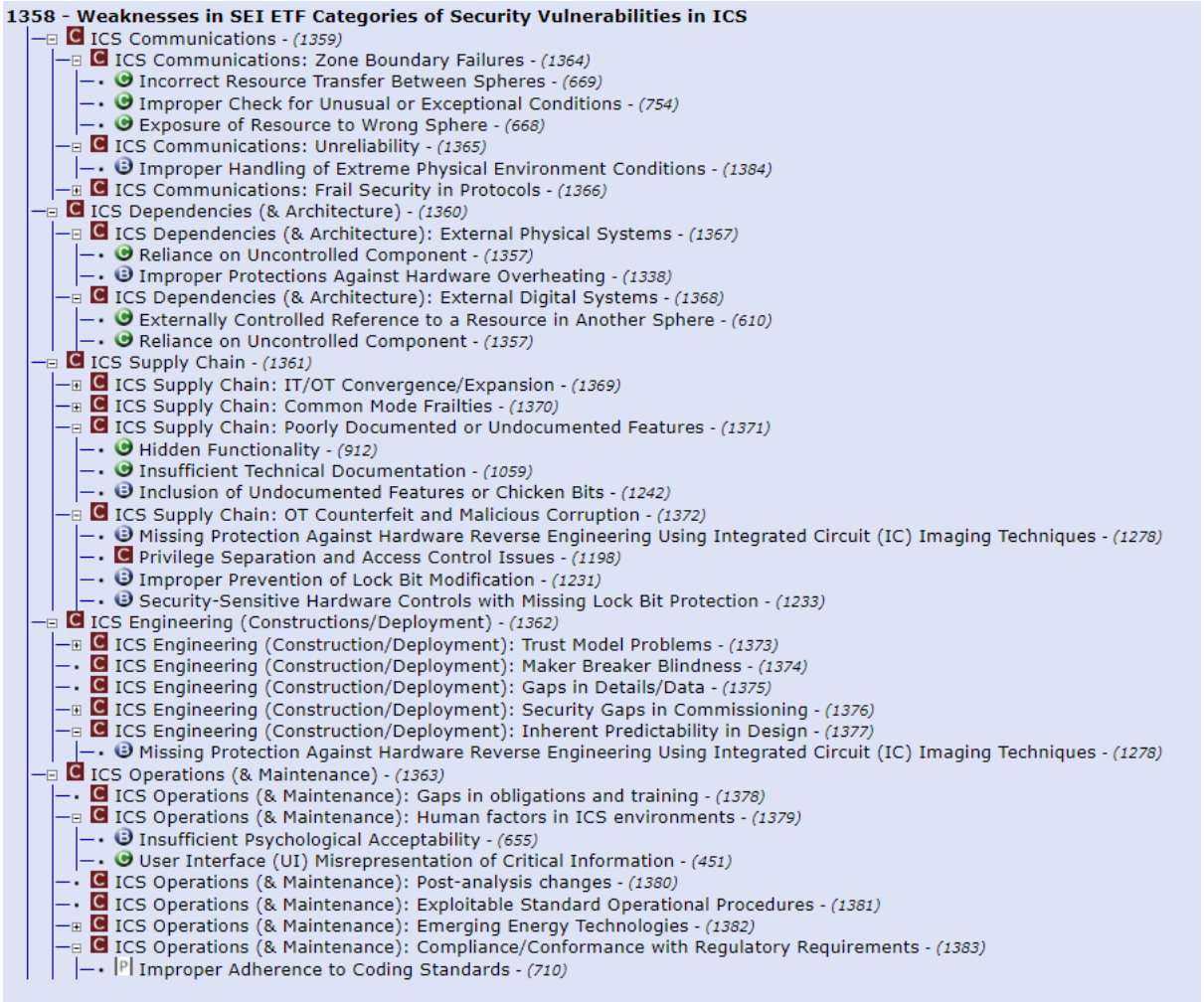
CWE 4.7 Release – Highlights Related to ICS/OT

- **Some content changes influenced by SEI ETF Categories document**
- **(New) CWE-1384: Improper Handling of Extreme Physical Environment Conditions**
  - NCSV 11. Maker Breaker Blindness
  - NCSV 16. Human factors in ICS environments
  - Parent of some existing CWEs
- **(Modified) CWE-1059: Insufficient Technical Documentation**
  - NVSV 8. Poorly documented or Undocumented features
  - Includes "gold standard"
  - Parent of some existing CWEs
- **(New) CWE-1357: Reliance on Uncontrolled Component**
  - NCSV 7. Common mode frailties
  - Parent of some existing CWEs

CWE 4.7 - New SEI ETF view

- **New view: CWE-1358: Weaknesses in SEI ETF Categories of Security Vulnerabilities in ICS**
  - https://cwe.mitre.org/data/definitions/1358.html
  - 3-level hierarchy ("super-categories", categories, weaknesses)
  - Currently includes all TPT-recommended mappings and MITRE's recommended mappings
  - Active development to take place in the coming months (in the SIG)
  - Many "scoping" challenges, e.g., human processes or practices
- **Signals new expansion / coverage of ICS/OT**
  - Possible overlap with hardware CWE, Top 20 Secure PLC Coding Practices

ICS/OT View – Sample Visualization



- This screenshot is partially expanded
- Red “C” icon = CWE Category
- Green “C” C / Blue “B” icons – Class/Base level weaknesses
- Categories without member weaknesses have a dot to the left of their icon
- Go to individual web page for CWE-1358
- Click “Expand All”

https://cwe.mitre.org/data/definitions/1358.html

Expansion of CWE-CAPEC scope to ICS/OT systems

- **CWE does not (yet) have formal definitions for its scope**
- **Primary scope: "mistakes in behavior of software or other electronic logic that has been shown - or can be reasonably expected – to contribute to real-world vulnerabilities"**
- **Focus: any measurable or analyzable artifact related to design, architecture, or other phase that (1) enables the introduction or (2) prevents the detection of weaknesses**
- **Scope expansion might require public debate**
  - CWE/CAPEC Board
  - SIGs (HW-SIG, ICS/OT SIG)
  - Other stakeholders (e.g., CWE-Research "power users," sponsor)

Expansion of CWE-CAPEC Scope – From Low-Hanging Fruit to Pie in the Sky

- **Some concerns are more easily expressed as attacks (CAPEC) than weaknesses (CWEs)**
- **Many technical weaknesses fit within CWE/CAPEC's current scope**
  - However, architecture and systems-of-systems problems are not covered well
  - Clarifying problems like Access Control can be difficult because of the variety of models and terms in use
  - Unclear when to create new entries for a technology type or function, versus adding ICS-specific details to existing higher-level entries
  - Supply chain has been difficult to integrate into CAPEC
- **Scope "exclusions" try to clarify issues with submissions**

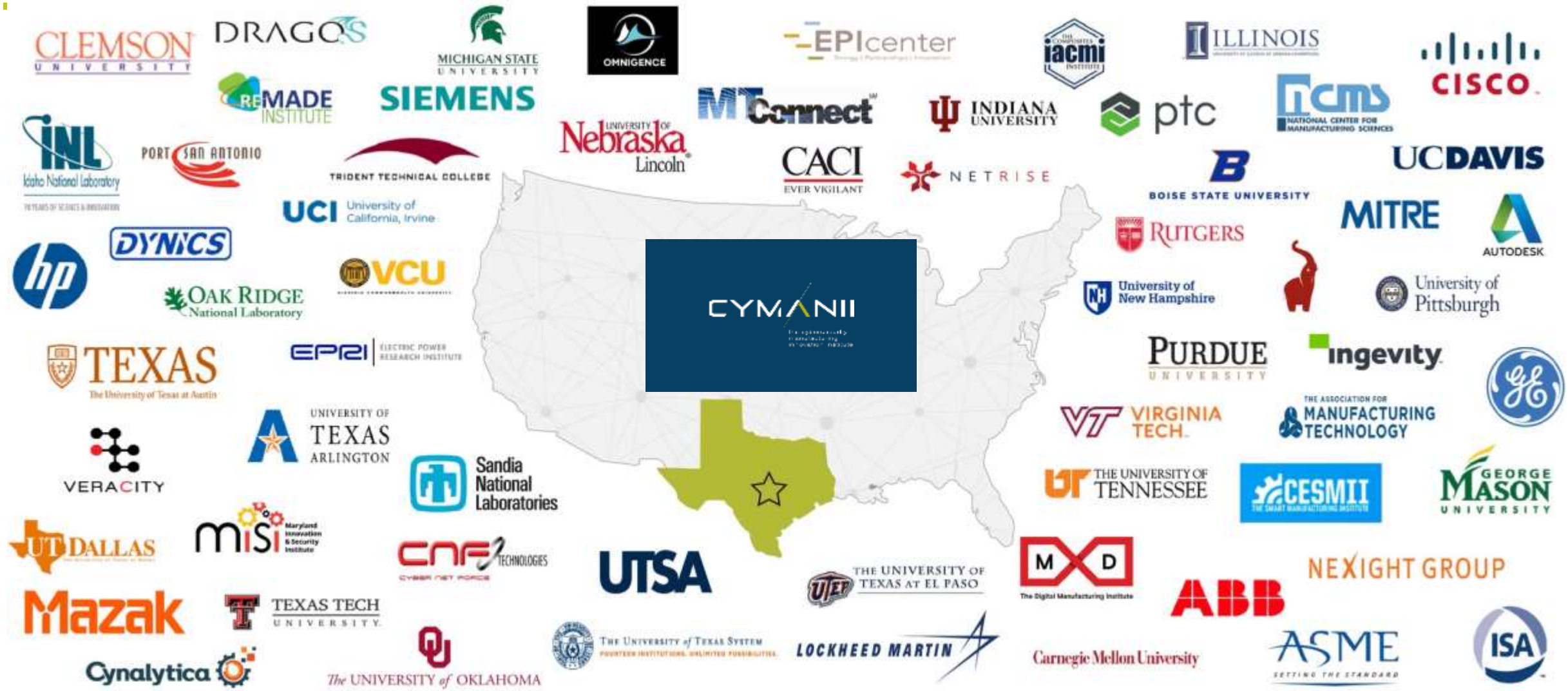
Examples of Scope Exclusions in NCSV TPT Paper

- **E2. Exclude any human or organizational process or policy that is not measurable and does not produce clear artifacts that identify weaknesses (BSIMM, NIST Secure Software Framework cover these)**
  - 13. Security Gaps in Commissioning
  - 15. Gaps in obligations and training
- **E4. Exclude conditions or situations in which weaknesses are more likely to appear**
  - 19. Emerging Energy Technologies
- **Detailed analysis of the paper to be conducted**
- **Draft scope exclusions to be sent to SIG**

Related Activities

CyManII Coordinated Vulnerability Awareness (CVA)

Cybersecurity Manufacturing Innovation Institute



We are threat informed.

All of our leadership, and most of our lead technical team, have TS/SCI clearances. Our technical work is driven by knowledge of threat vectors and how they are operationalized in manufacturing environments.

We develop inside a secure infrastructure.

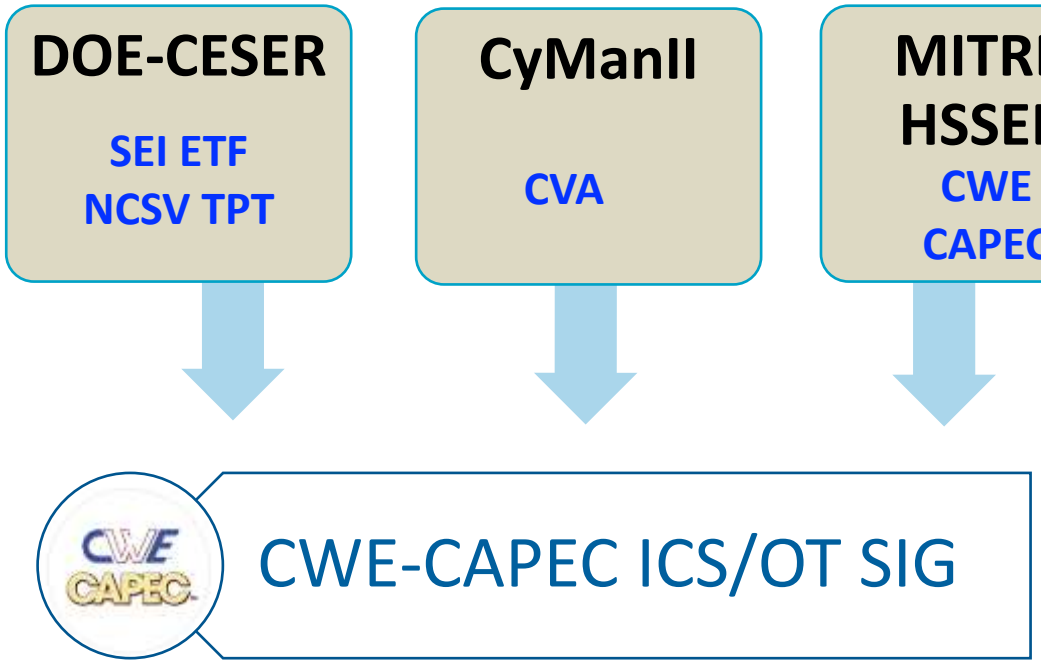
This infrastructure not only generates "secure by design" cyber products but does so in a secure build chain.

- Pervasive
- Unobtrusive
- Resilient
- Economical

We deploy CIE (cyber informed engineering) approaches.

We apply state-of-the-art CIE approaches as we design Secure Manufacturing Architectures (SMA).

Relationships

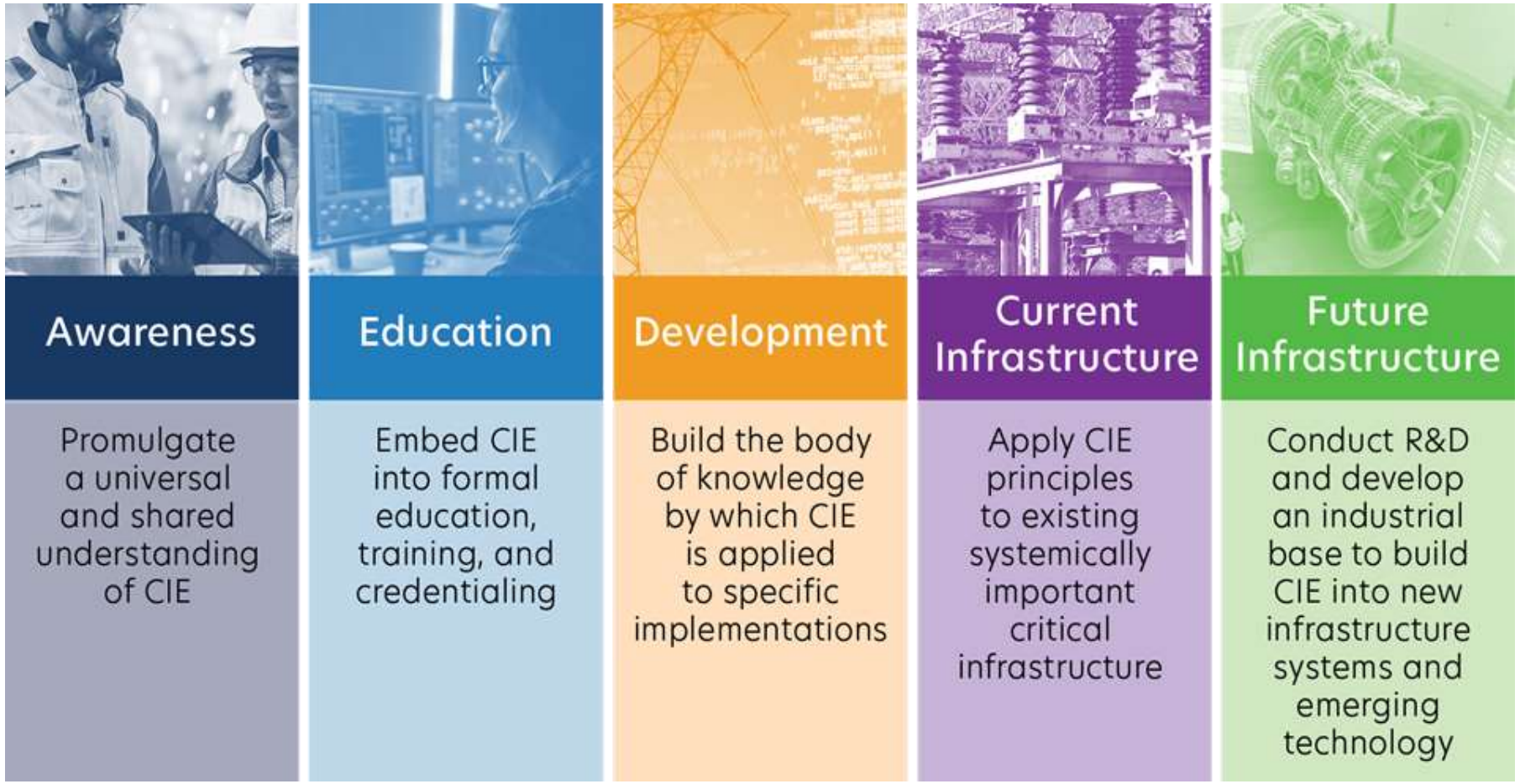


DOE	•Department of Energy
CESER	•Cybersecurity, Energy Security, and Emergency Response
SEI ETF	•Securing Energy Infrastructure Executive Task Force
NCSV	•New Classes of Software Vulnerability
TPT	•Technical Program Committee
CyManII	•Cybersecurity Manufacturing Innovation Institute
ICS/OT	•Industrial control systems/operational technology
CVA	•Coordinated Vulnerability Awareness
CWE	•Common Weakness Enumeration
CAPEC	•Common Attack Pattern Enumeration and Classification
SIG	•Special Interest Group

Coordinated Vulnerability Awareness (CVA)

- Goal: Build awareness and well-informed means of responding to reported vulnerabilities for a cyber-proactive manufacturing community
- DOE Requirement: Stakeholder driven, especially industry
- Progress to date
  - A "categorical" approach to identifying, preventing, mitigating vulnerabilities
  - Participation in the SEI-ETF working groups, especially NCSV
  - Drafting paper for IEEE Security & Privacy on the NCSV results
  - Established the Manufacturing Information Sharing and Analysis Center (M-ISAC) in collaboration with the Global Resilience Federation (GRF)

Cyber Informed Engineering (CIE)



For more information, visit: https://inl.gov/cie/

Where We Want to Go This Year

Work Plan

1. Review NCSV TPT work and prioritize/edit categories for incorporation into future CWE and CAPEC updates
2. Collaborate with MITRE to meet content submission requirements
3. Explore 2 categories/weaknesses for broader advisories/publications
4. Explore further avenues for dissemination/communication around weaknesses
5. Define current CWE/CAPEC scope
6. Identify challenges for expanding CWE/CAPEC scope

Major Milestones

- **CWE/CAPEC publish content on quarterly basis**
  - Next board meeting June 3, occurring quarterly
  - Next major update for CWE/CAPEC weakness Fall 2022

SIG Meeting Cadence

- **Start with monthly meetings – third Wednesday of each month?**
  - Wed 6/15 @ 3pm ET?
- **Consider less frequent meetings after first three meetings**

Wrap-Up

Next Steps

- **Request access to the public & private Github repositories for the ICS/OT SIG**
- **Review the 20 categories of security vulnerabilities identified in the SEI ETF**
- **Respond to request to provide feedback on the ICS/OT SIG work plan**
- **Look for calendar invite for next meeting. Think about meeting cadence and structure.**

MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Learn more www.mitre.org