# CWE-CAPEC ICS/OT Special Interest Group

## Wednesday, June 29, 2022

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

# ICS/OT Special Interest Group Participants

1. **Aagam Shah**
2. **Aamir Khan,** Tata Power
3. **Abdelrahman Elsanose**
4. **Adam Hahn**
5. **Adrian Crespo-Ortiz,** Capgemni
6. **Ahmad Sharafi,**
7. **Albert Vartic,** OMV Petrom
8. **Alex Rodriguez**, PG&E
9. **Alfinie Bullock,**
10. **Amanda Kraus**
11. **Andres Fuentes-Fernandez,** Inetum
12. **Andrew Kling**, Schneider Electric
13. **Andy Kling,** Schneider Electric
14. **Anton Shipulin**
15. **Armada Sramek**
16. **Ashley McGlone**, Tanium
17. **Aw Landgraaf,**
18. **Ayman Alissa**, Mckinsey
19. **Barry Greene**, Senki
20. **Bayard Johnson**
21. **Bill Newhouse**
22. **Brandon Carter**,
23. **Ben Deering,** ODNI
24. **Ben Sooter**, EPRI
25. **Beverly Novak**, INL
26. **Bill Aubin**, Nozomi Networks
27. **Bill Kintz**, Invictus
28. **Bill Newhouse**
29. **Bob Hanson,** LLNL
30. **Bob Heinemann,**
31. **Bob Radvanovsky**
32. **Bradley Nickens**, GE
33. **Bryan Beckman,** INL
34. **Bryan Owen**, Aveva
35. **Cameron Burden,**
36. **Carl Mccants,** ODNI

# ICS/OT Special Interest Group Participants

37. **Carmen Zapata**, DHS
38. **Chris Charpentier**, GE
39. **Christopher Havey,** Applied Cybersecurity Engineering
40. **Christopher Sundberg**, Woodward
41. **Chris Humphrey**, Boeing
42. **Chris Levendis**,
43. **Cody Kieltyka**,
44. **Craig Barrett,** Kinder Morgan
45. **Curtis Taylor**, CyManII
46. **Curt Wiggins**
47. **Cynthia Hsu**, DOE
48. **Dana Thomas**
49. **Dan Bennett,** NREL
50. **Dan Ehrenreich,** SCCE
51. **Danielle Jablanski**,
52. **Daniel Santos**, Forescout
53. **Daniel Stachan**
54. **Daryl Haegley**
55. **Dave Halla**
56. **Dave Keppler**
57. **David Nicol**, UIUC & CyManII
58. **David Simpson**
59. **Deborah Kobza,** IACI
60. **Derek Hart**
61. **Dimple Shah**
62. **Dylan Sundy**
63. **Ed Hicks**
64. **Eric Cosman**
65. **Eric Mitchell,** NSA
66. **Eric Strief,** John Deere
67. **Erik Hrin**
68. **Espen Endal,** KraftCERT
69. **Evgeni Sabev**
70. **Gananand G Kini**
71. **Greg Ahira,** GE
72. **Greg Bastien**

# ICS/OT Special Interest Group Participants

73. **Greg Sanchez**
74. **Gus Serino**
75. **Hadeli Hadeli,** Hitachi Energy
76. **Haritha Srinivasan,** FM Global
77. **Harry Perper,** Cyber Architecture and Resiliency
78. **Howard Grimes,** CyManII
79. **Iain Deason,** DHS CISA
80. **Ismael Garcia,** NRC
81. **Jace Powell,** Fortress
82. **Jarvis Robinson**
83. **Jason Li,** TrustedST
84. **Jason Plant**
85. **Jay Gazlay,** DHS CISA
86. **Jen Walker,** Water ISAC
87. **Jennifer Pedersen**
88. **Jeremy Mckeown**
89. **Jesper Johansson,** Nouryon
90. **Jess Smith,** PNNL
91. **Jodi Jensen**
92. **Joe Agres,** West Yost
93. **Joe McCormick**
94. **Joe Weiss**
95. **John Almlof**
96. **John Kingsley**
97. **John Schneider**
98. **John Parmley,** Zuuliot
99. **John Ransom**
100. **Jon Terrell,** Hitachi Energy
101. **Jon White,** NREL
102. **Jonti Talukdar,** Duke
103. **Jordon Sims**
104. **Jose Jimenez,** Sothis
105. **Jose Perez,** Tenable
106. **Joseph Cummings,** NYPA
107. **Joseph Januszewski,** E-Isac
108. **Joseph Matthews**
109. **Jude Desti,** Boeing
110. **Justin Cain**

# ICS/OT Special Interest Group Participants

111. **Karen Wetzel**
112. **Ken Wang,** DOD
113. **Kerry Stuver,** GE
114. **Khalid Ansari,** FM Approvals
115. **Kimberly Denbow,**
116. **Krystel Castillo**
117. **Kumar**
118. **Kyle Johnson,** GSOC
119. **Lindsey Cerkovnik,** DHS CISA
120. **Marc Sachs,** Auburn University
121. **Mark Sullivan,** NSA
122. **Martijn Jansen,** Taqa
123. **Martin Kihiko**
124. **Martin Ring,** Bosch
125. **Martin Scheu,** Switch
126. **Marty Edwards**
127. **Matt Bishop,** UC Davis & CyManII
128. **Marie Stanley Collins**
129. **Matthew Bohne**
130. **Matthew Knoll,** ArcelorMittal
131. **Max Wandera,** Eaton
132. **Megan Samford**
133. **Melissa Vice,** Air Force
134. **Michael Chaney,** CyManII
135. **Michael Hok,** Hitachi Energy
136. **Michael Toecker**
137. **Michalis Pavlidis,** University of Brighton
138. **Monika Akbar,** UTEP & CyManII
139. **Muhammed Shaban**
140. **Nik Urlaub**
141. **Niyu Ogunniyi,** Corteva
142. **Oystein Brekk-Saunderud,** Norma Cyber
143. **Patrick Dale**
144. **Patrick Obruba**
145. **Patti Escatel,** DHS CISA
146. **Paul Martyak,** EPRI
147. **Paul Peix,** Headmind

# ICS/OT Special Interest Group Participants

148. **Paul Zawada**
149. **Pete Tseronis**
150. **Peter Colombo**
151. **Peter Jackson,** SGS
152. **Peter Pongracz** (Added)
153. **Philip Huff, UALR**
154. **Pierre Janse van Rensburg,** BBA
155. **Piotr Pedziwiatr,** Arcelor Mittal
156. **Ralph Ley**
157. **Raymond Savarda**
158. **Renan**
159. **Rex Wempen,** DOE
160. **Rezaur Rahman**
161. **Rich Piazza**
162. **Richard Robinson,** Cynalytica
163. **Rita Ann Foster** (Added)
164. **Robert Garry,** GE Gas Power
165. **Robert Heinemann**, MITRE
166. **Robert Murphy**
167. **"Rob"** (Added – Unsure which of the above)
168. **Roger Johnson,** Novelis
169. **Ronald Atwater**
170. **Ryan Bays,** PNNL

169. **Ryan Gagliastre,** HF Sinclair
170. **Sabri Khemissa**
171. **Sachin Shah,** Armis
172. **Saleh Almaghrabi**
173. **Salman Salman,** Aerospace Corporation
174. **Sam Blackfell**
175. **Samuel Chanoski,** INL
176. **Sandeep Shukla,** Virginia Tech
177. **Sarah Fluchs,** Admeritia
178. **Shane Stailey**
179. **Shannon Hughes**
180. **Shadya Maldonado,** INL (Added)
181. **Sharin Crane,** Boeing
182. **Sharla Artz**
183. **Sherry Hunyadi**
184. **Steve Battista**
185. **Steve Chapin**
186. **Steve Granda,** NREL
187. **Stephanie Saravia**
188. **Stephen Trachian,** Hitachi Energy
189. **Susan Farrell, ObjectSecurity** (Added)

# ICS/OT Special Interest Group Participants

189. **Ted Wittmer**
190. **Thomas Ruoff,** DHS CISA
191. **Timothy Isaacs,** NuScale Power
192. **Todd Riley, Goodyear**
193. **Tom McGoogan**
194. **Tony Turner,** Fortress
195. **Tonya Riley,** Cyberscoop
196. **Tracy Briggs,** CyManII
197. **Travis Ashley,** PNNL
198. **Vivek Ponnada**
199. **Wayne Austad,** CyManII
200. **Wayne Cantrell**
201. **William Kintz** (Added)
202. **William Welch**
203. **Yasoda Ramchune,** Chevron
204. **Zachary Rogan,** Xage

# ICS/OT Special Interest Group Leadership and Support

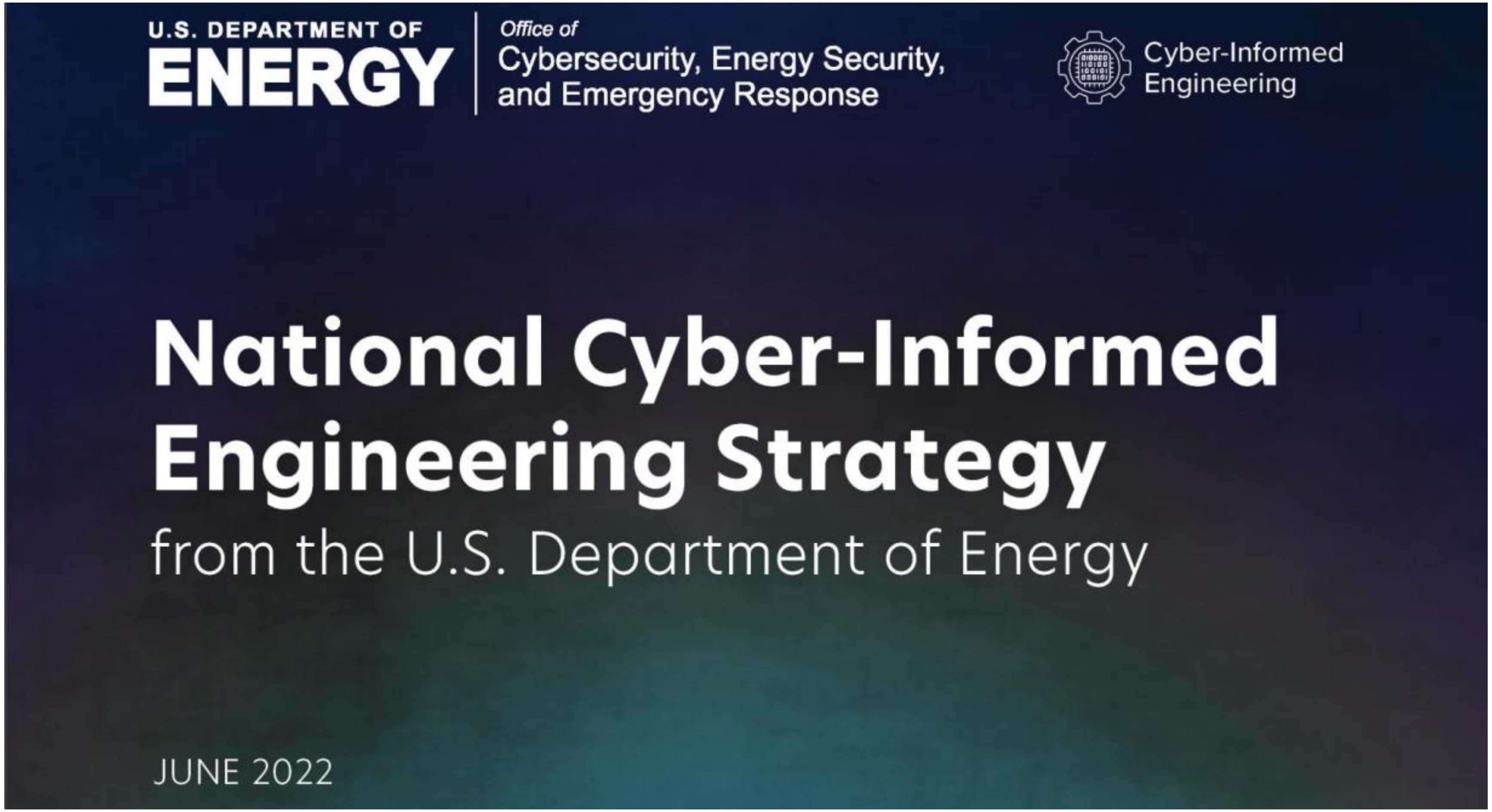
1. **Alec Summers**, MITRE
2. **Andrew Kresses**, Nexight Group
3. **Cheri Caddy,** DOE-CESER
4. **Daisyareli Martin**, Nexight Group
5. **Greg Kerr**, Nexight Group
6. **Greg Shannon**, CyManII
7. **Ginger Wright,** INL
8. **Jeff Hahn,** INL
9. **Jeff Mitchell,** INL
10. **Jennifer Ekperigin**, Nexight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

# Agenda

| Eastern Time | Activity |
|---|---|
| **3:00 – 3:05 pm** | **Login and Roll Call** |
| **3:05 – 3:15 pm** | **Opening Remarks**<br>• Overview of National CIE Strategy announcement<br>• Overview of SIG plans going forward |
| **3:15 – 3:35 pm** | **CWE-CAPEC Current Scope**<br>• Defining the current scope<br>• Discussing challenge areas |
| **3:35 – 4:05 pm** | **Breakout Sessions**<br>• Topic 1: Defining the set of stakeholders<br>• Topic 2: Identifying what gaps participants think would be useful for this working group to address |
| **4:05 – 4:25 pm** | **Group Discussion**<br>• How does the SIG influence CWE/CAPEC? What are the formal/informal mechanisms?<br>• How awareness of CWE/CAPEC be improved/expanded? What additional avenues for dissemination/communication around weaknesses are available? |
| **4:25 – 4:30 pm** | **Wrap-Up**<br>• Closing remarks<br>• Forming a working group by summer<br>• Next SIG meeting – Wed 7/27 @ 3pm<br>• Action Items |
| **4:30 pm** | **Meeting Ends** |

# Opening Remarks

# National Cyber-Informed Engineering Strategy



U.S. DEPARTMENT OF ENERGY

Office of Cybersecurity, Energy Security, and Emergency Response

Cyber-Informed Engineering

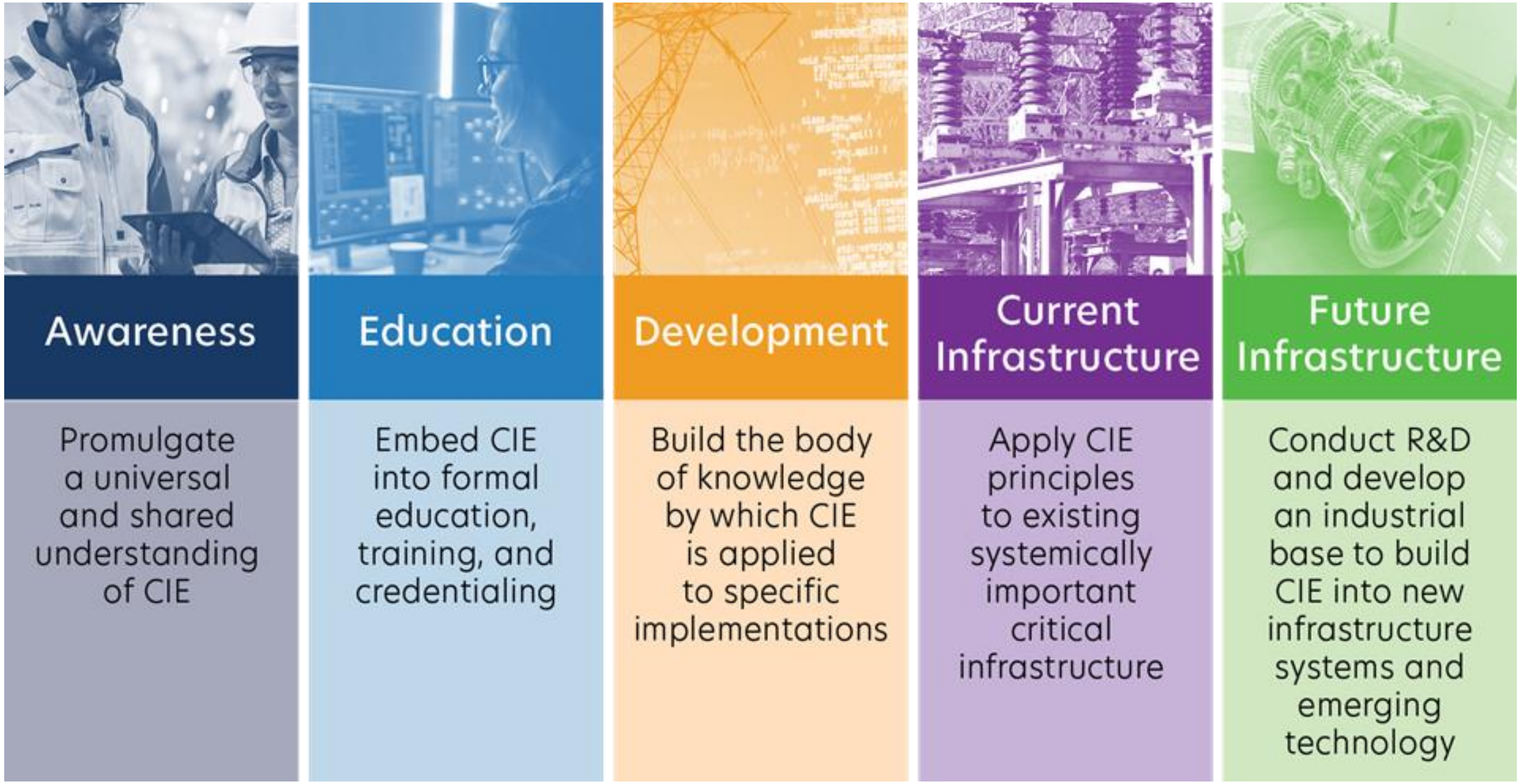
National Cyber-Informed Engineering Strategy

from the U.S. Department of Energy

JUNE 2022

**URL:** https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document

# Cyber Informed Engineering (CIE)



| Awareness | Education | Development | Current Infrastructure | Future Infrastructure |
|---|---|---|---|---|
| Promulgate a universal and shared understanding of CIE | Embed CIE into formal education, training, and credentialing | Build the body of knowledge by which CIE is applied to specific implementations | Apply CIE principles to existing systemically important critical infrastructure | Conduct R&D and develop an industrial base to build CIE into new infrastructure systems and emerging technology |

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

# Work Plan/ *Current Activities*

1. **Review NCSV TPT work and prioritize/edit categories for incorporation into future CWE and CAPEC updates**
   - *Identifying next tranche of SEI ETF categories for CWE-CAPEC updates*
2. **Collaborate with MITRE to meet content submission requirements**
   - *Requirements defined; submission process iterative*
3. **Explore 2 categories/weaknesses for broader advisories/publications**
4. **Explore further avenues for dissemination/communication around weaknesses**
   - *Discussion topic for today*
5. **Define current CWE/CAPEC scope**
   - *Read-ahead sent on current scope*
6. **Identify challenges for expanding CWE/CAPEC scope**

# CWE Scope and Scope Exclusions

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

# Observation: CWE is Already Useful for Many ICS/OT Vulnerabilities

- **CWE already covers many design-related issues**
- **OT:ICEFALL (Forescout) – 56 "insecure-by-design" vulnerabilities**
  - No CWE mappings
  - Hardcoded credentials (CWE-798)
  - Hardcoded crypto key (CWE-321)
  - Plaintext transmission (CWE-319)
  - Weak encryption (CWE-327)
  - No authentication (CWE-306)
  - … and many more
- **Experimental custom Top-N list for all ICS-CERT advisories shows same kinds of issues, plus buffer overflows, injection, etc.**
- **CWEs do not have ICS-specific examples or metadata saying they apply to ICS**

# The NCSV TPT Categories Include “Gaps” for CWE to Address

- **Which “gaps” are specifically about weaknesses (coding mistakes)?**
- **Which “gaps” are related to other phases of the Secure Development Life Cycle?**
  - Operations / system administration
  - Policy
- **Some categories may be orthogonal to weaknesses, or effectively cover all known weaknesses**
- **Defining CWE’s “Scope” and characterizing difficulties in external submissions is actively underway.**

# Expansion of CAPEC-CWE 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 CAPEC-CWE 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**

# Proposed Scope Exclusions

- Clarify commonly-seen problems in CWE submissions
- Decision is not final yet - focus discussion and debate, increase transparency/tracking
- Submissions with these issues can’t receive a CWE ID, but might be captured within fields
- SEI ETF “20 Categories” document issues highlighted in yellow

| | Description |
|---|---|
| E1 | Any mistake that has not and cannot happen within real-world software or other electronic logic. |
| E2 | Any human or organizational process or policy that is not measurable and does not produce clear artifacts that identify weaknesses, such as training or testing. Rationale: weaknesses can emerge as a result of these activities; BSIMM, OpenSAMM, NIST Secure Software Development Framework, etc. already cover this area. |
| E3 | Any characterization of motivation (e.g., “malicious”) that does not focus on the actual mistake, whether intentionally or accidentally introduced. Rationale: a weakness is based on the behavior of the product. |
| E4 | Conditions or situations in which weaknesses are more likely to appear. Rationale: these are modes of introduction, which is a separate field in a CWE entry. |

# Proposed Scope Exclusions (2)

- Other exclusions might be added

| | Description |
|---|---|
| E5 | Any collection of groupings related to the same technology, same language, development lifecycle, etc., without a common behavior. Rationale: weaknesses are based on specific behavior. Such items could be a category. |
| E6 | There is no actionable mitigation available to the developer to prevent or reduce the weakness. |
| E7 | The issue is not relevant to the threat model / security concerns of product’s owner/operator (i.e., the customer). |
| E8 | The issue does not directly conflict with other CWE entries, e.g., “X is bad” in one CWE, and “Y is bad so do X instead” in another CWE. |
| E9 | (NEW) The issue is not solely related to safety or reliability, i.e., it must be somehow related to security. (Clarification on privacy – if an issue is related to desires for access control or preservation of confidentiality, it is within scope of “security”). Rationale: many aspects of industrial safety, such as correct electric shielding and insulation, are not affected by security. |

# 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 and shared**
- **Draft scope exclusions to be sent to SIG**

# Characterizing Submission Problems

- Even if a submission covers a weakness, it may be difficult and time-consuming to integrate it into CWE
- Each submission might be labeled with one or more “complications” to facilitate tracking
- Main problems in original “submissions” from SET ETF highlighted in yellow

| | Description |
|---|---|
| P1 | Duplicates or partial overlaps with existing weaknesses, either indicating problems with the submission, existing CWE entries, or CWE’s “vulnerability theory” model of weaknesses |
| **P2** | Abstraction is either too high-level or too low-level |
| **P3** | Weakness not well-described (lots of back-and-forth) |
| **P4** | Bare-bones submissions (team has to create or provide lots of extra data) |
| P5 | Concerns with intellectual property rights |

# Breakout Sessions

# Breakout Session 1 – Facilitated by Greg Kerr

**Topic 1: Defining the set of stakeholders**

- Vendors, Product Developers, Integrators, End Users (utilities, etc.), Researchers, Someone from Acquisitions to ensure proper terminology.
- Vendors from standards like ISA 62443, IEC, CISA (ICS-CERT, US-CERT), NIST
- What is equivalent for ISAC or CERT for those designing new products/ methods/ validation techniques? Is there a new community besides standards bodies on how to defined and eliminate weaknesses?
- Have plenty in place for backside, but not on proactive side.
- All levels of management – give different perspectives. ISAC representatives. Policy.
- Want to ensure CWE are both human and machine readable.

## Topic 2: Identifying gaps participants think would be useful for this working group to address

- General: weaknesses drive out creation of vulnerabilities. About physical and engineering context that others do not address.
- Weaknesses are about being more proactive.
- Conflicting priorities. Balancing between quality outcome vs. cost and time. (acceptable risk vs. outcomes)
- End owner of weakness/vulnerabilities need to make consequence/risk decisions.
- Communications challenge: end user doesn't know they have weakness/vulnerability. Recognize how they digest it.
- We should determine how we affect these activities (SBOM, etc.)
- We should structure activities to make it easier for ISAC to communicate weaknesses.
- Success measure: impact secure design lifecycle tools / practices.

# Breakout Session 2 – Facilitated by Katie Baker

## Topic 1: Defining the set of stakeholders

- ICS Asset Mans. – **collaborative testing and sharing may reduce CWEs becoming CVEs**
  - Electrical, Water, ONG, etc.
- Software security tool manufacturers/(vendors?)
  - Purdue levels 1-3
  - DevSecOps vs ISV
- Supply chain for manufacturers
  - Chip and software
- Manufacturers of discreet components
- Security Researchers
- AOOs for each CI sector – critical path for operations (what must be maintained to operate)
- OSS community – widely used, can be more proactive re: CWEs
- Other OT SIGs (ISA, CS2AI, etc) – see where we can cross-pollinate.

Rep types:

- Chief Engineers, Lifecycle specialist, CTOs, Product Managers (R&D), CISO, SBOM/HBOM specialists.

## Topic 2: Identifying gaps participants think would be useful for this working group to address

- Critical path – identifying how specific equipment, components, etc are manufactured/dev/programed. Prioritization. Measured approach to identify criticality.
- Resilience measurement
- systemic approach for investing to reduce losses associated with addressing issues.
- **Education – inform SANS/ICS classes or other education opportunities. Both existing workforce and pipeline.**
  - Provide a tangible result – maybe a tool to navigate the CWEs and assess impact
- Culture – awareness of real risk and your role in reducing that risk. Proactive vs reactive
- Tracking mitigation of CWE such as those identified by CyTRICS (are they fixed or simply identified) – progress metric

# Breakout Session 3 – Facilitated by Daisyareli Martin

## Topic 1: Defining the set of stakeholders

- Owner operators across several different ICS domains seem to have a different role than traditional IT in the IT environment
- Equipment vendors and system integrators that deliver integrated systems to the end users and operator/owners
- Certification labs – gap
- Academic community – opportunity to develop research that center around the different stages of CWE (uses, effectiveness, gaps, proposed ideas, etc.)
- Those who might be responsible for reporting "mistakes"
- Attorneys and the legal community + Insurance Community
  - Shaping policy direction – these stakeholders only come in when something bad happens so having their insight may be useful in shaping policy directions.
- Consultants - form trust relationships and need configuration
- Market analyst community
- Engineers, Operators, Technical managers
- Integrators

## Topic 2: Identifying gaps participants think would be useful for this working group to address

•There are vulnerabilities that can be identified by different entities however to resolve and or start working on the OT cyber issue, we need to look at the manufacturers. Not only by mandating vulnerability reporting, but also by improving the architecture of their solutions

•A lack of awareness in the ICS/OT community – many of the owner operators lack awareness of some the basic laws and the components being used and how flawed the security profiles are

•There is IT communication vectors, but we don’t know what the right ICS/OT communication vectors are for disseminating information

•One way street in disseminating information without having some type of acknowledgment that the concern was received by the end user and any necessary steps were taken to either mitigate the vulnerability or weakness or verify that it was not relevant to the application that was being applied to the end user.

• Need formotionable vetting on the CWE side – not anything close to what has been done on the vulnerabilities side (CVE)

•What are the barriers the receiving audience facing that either is resistance or reluctant or unable to receive the information? An enormous amount of information is being pushed out to some of these target audiences and for whatever reasons that we may or may not understand, they’re not taking that information on and taking actions

# Breakout Session 4 – Facilitated by Andrew Kresses

**Topic 1: Defining the set of stakeholders**

- System/software developers
- Security architects
- Auditors/assessors ISSOs ISSMs
- Security engineers tasked with implementation
- General vulnerability/risk management
- Software quality assurance
- Firmware developers x2
- Security analysts/researchers
- Dev-sec Ops
- Infrastructure security specialists
- AOOs
- Vendors
- Red team and pen testers

**Topic 2: Identifying gaps participants think would be useful for this working group to address**

- Prioritization of CWE
- Are the stakeholders aware of where to find the information that they need? Are they getting it?
- How does a CWE tie into a CAPEC tie into a CVE? The digital thread?
- How does att&ck tie into related frameworks?
- The distinction between code and infrastructure weaknesses. How do you differentiate?
- The d3fend framework and tying these into this process.
- Connecting CWE to the CIE framework.
- Education on the differences between CWEs (tied to point 2)
- Rapid, cloud-driven software development and how this changes the mindset
- Cyberphysical development as well

# Breakout Session 5 – Facilitated by Jennifer Ekperigin

## Topic 1: Defining the set of stakeholders

- Research groups and third-party cybersecurity companies (Dragos, Honeywell, Schneider, Claroty, Bechtel, GE, Nozomi, Schweitzer, Siemens, Xylem, Rockwell, Johnson Controls, CyPhy, Nova, Munio)
- Academic Affiliations (specifically, anyone with a lab that can help process data and put it into terms that all other industry stakeholders can understand. Other educators should also be included, however, such as those pursuing PhD in the field and others that comprise the upcoming wave of talent entering the industry as they are likely to propose novel ideas untainted by how things are traditionally done)
- Community involvement at all industry levels (engineers, software developers, security specialists, AOOs, technical experts, leaders/managers, analysts, researchers, hardware/device manufacturers, engineers, vendors)
- Policymakers (attorneys, local representatives)
- Individuals from other sectors who have successfully resolved similar security concerns – What are they doing and how can we implement those same solutions here?

## Topic 2: Identifying gaps participants think would be useful to address

- Utilization of CWE/normalization of data (data is elusive and we need to compare apples to apples, by putting it into terms we can all understand)
- Effort should be put into identification of attack patterns (so that data can be utilized in a way we can each apply to our individual/unique environments)
- Better communication both among industry stakeholders and between the industry and academic consortia (those who can collect real-time data and those who can process and make meaning of that data for us to apply).
- It's an ever-evolving field, and it's expensive to do detection and collect data. It needs to be more obvious what the problems are at all levels (right now there is a profound lack of awareness) and solutions need to be more accessible (i.e., more affordable)
- Emerging tech is challenging the existing legacy understanding of and approach to the data and we need to know how to utilize the new technology available in a meaningful way (which is why including academia and incoming talent is vital)
- OT devices were not built for the load they are expected to now carry. Updates not only need to be accessible to the industry, but someone needs to actively push those updates on the industry to make them aware of their importance.

# Group Discussion

# Questions

- **How does the SIG influence CWE/CAPEC? What are the formal/informal mechanisms?** *(for MITRE)*
- **How does this group want to influence CWE/CAPEC?**
- **How can awareness of CWE/CAPEC be improved/expanded?**
- **What additional avenues for dissemination/communication around weaknesses are available?**

# Wrap-Up

# Question for the group

- **Does anyone object to including your name and organization in the ICS/OT SIG meeting minutes?**

# Major Milestones

- **ICS/OT SIG meets monthly**
  - Next meeting Wednesday 7/27 from 3:00 to 4:30pm ET
- **CWE/CAPEC publish content on quarterly basis**
  - Next board meeting [TBD, sometime in September], occurring quarterly
  - Next major update for CWE/CAPEC weakness Fall 2022

# Action Items

1. **Request access to the public & private Github repositories for the ICS/OT SIG**
2. **Review the 20 categories of security vulnerabilities identified in the SEI ETF**
3. **Respond to flash survey (via QuestionPro) to provide feedback**
   - ICS/OT SIG work plan
   - Suggesting a sub-working group
     - Identifying activities, purpose, and outcomes

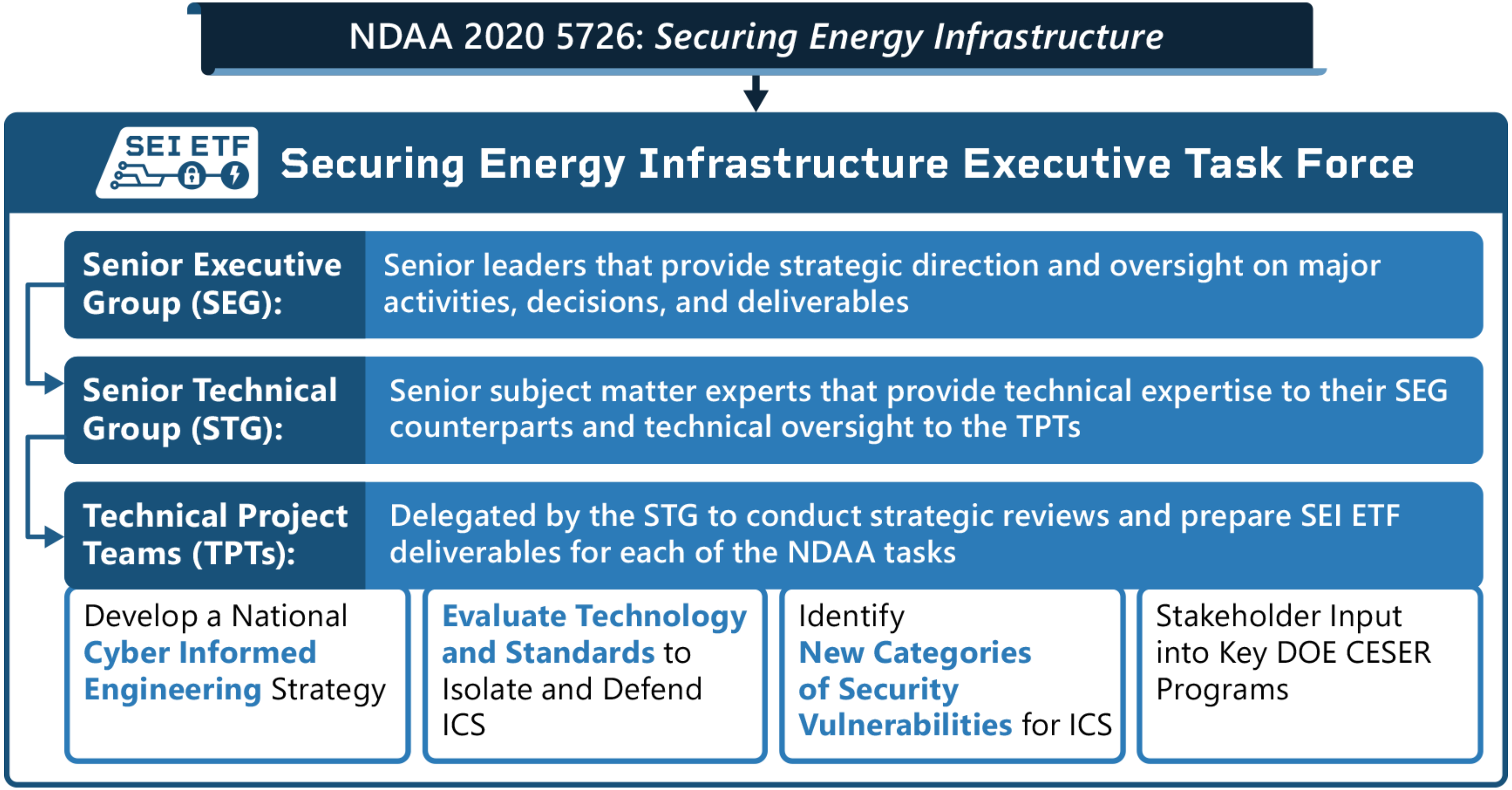
MITRE

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

# Additional Program Background

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



NDAA 2020 5726: *Securing Energy Infrastructure*

**Securing Energy Infrastructure Executive Task Force**

**Senior Executive Group (SEG):** Senior leaders that provide strategic direction and oversight on major activities, decisions, and deliverables

**Senior Technical Group (STG):** Senior subject matter experts that provide technical expertise to their SEG counterparts and technical oversight to the TPTs

**Technical Project Teams (TPTs):** Delegated by the STG to conduct strategic reviews and prepare SEI ETF deliverables for each of the NDAA tasks

- Develop a National **Cyber Informed Engineering** Strategy
- **Evaluate Technology and Standards** to Isolate and Defend ICS
- Identify **New Categories of Security Vulnerabilities** for ICS
- Stakeholder Input into Key DOE CESER Programs

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

**KEY DELIVERABLE:**

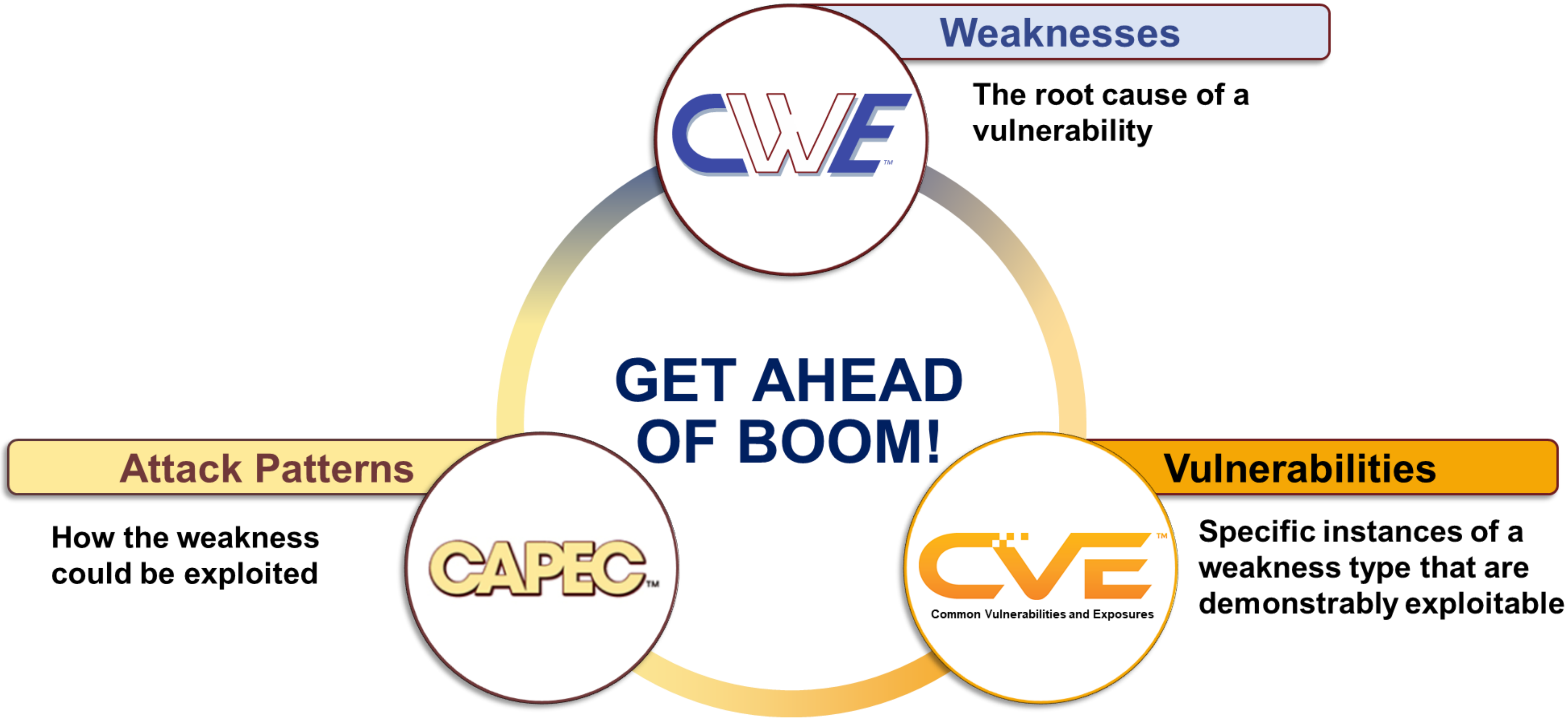
**Categories of Security Vulnerabilities in ICS**

- 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



**Weaknesses**

The root cause of a vulnerability

**Attack Patterns**

How the weakness could be exploited

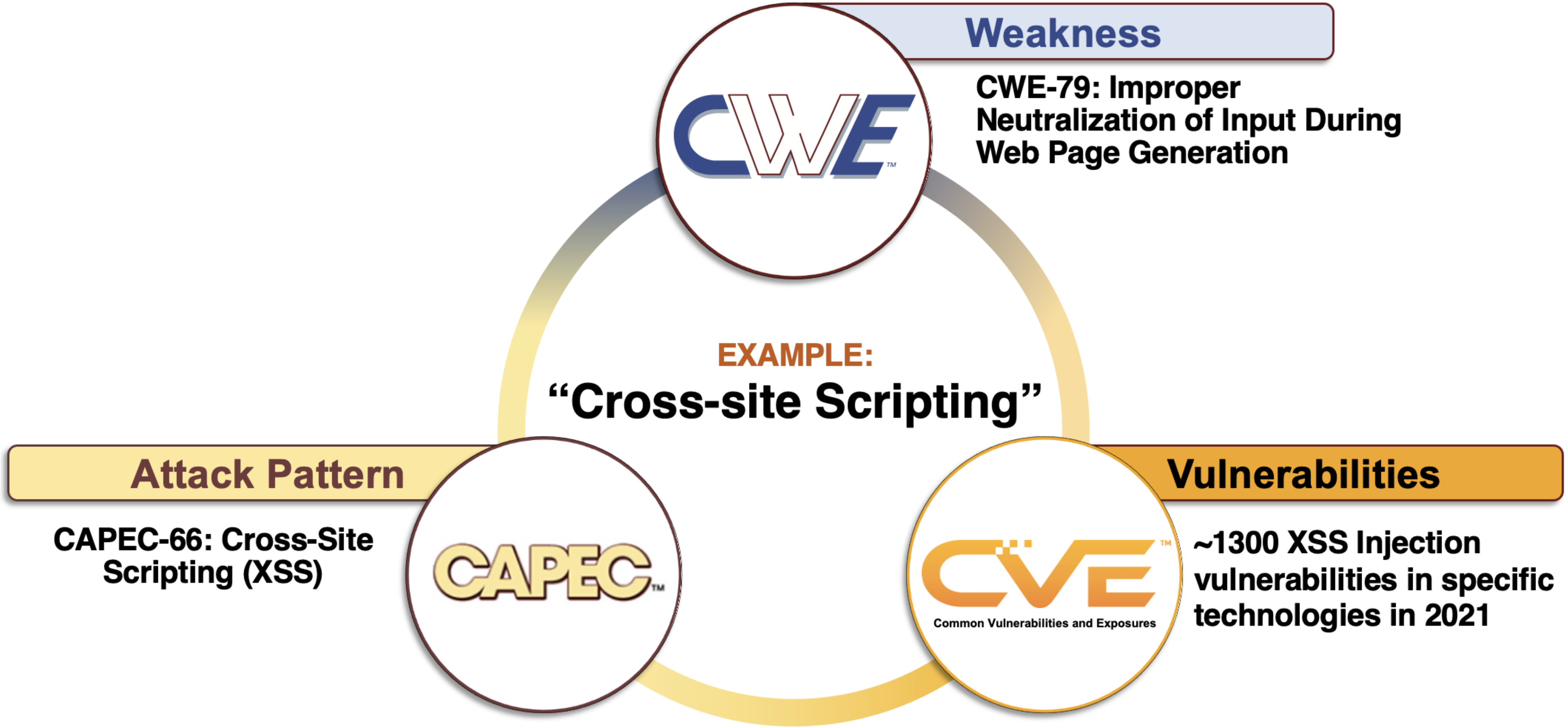
**GET AHEAD OF BOOM!**

**Vulnerabilities**

Specific instances of a weakness type that are demonstrably exploitable

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

# ‘Get Ahead of Boom’ Landscape



Weakness

CWE-79: Improper Neutralization of Input During Web Page Generation

EXAMPLE:

“Cross-site Scripting”

Attack Pattern

CAPEC-66: Cross-Site Scripting (XSS)

Vulnerabilities

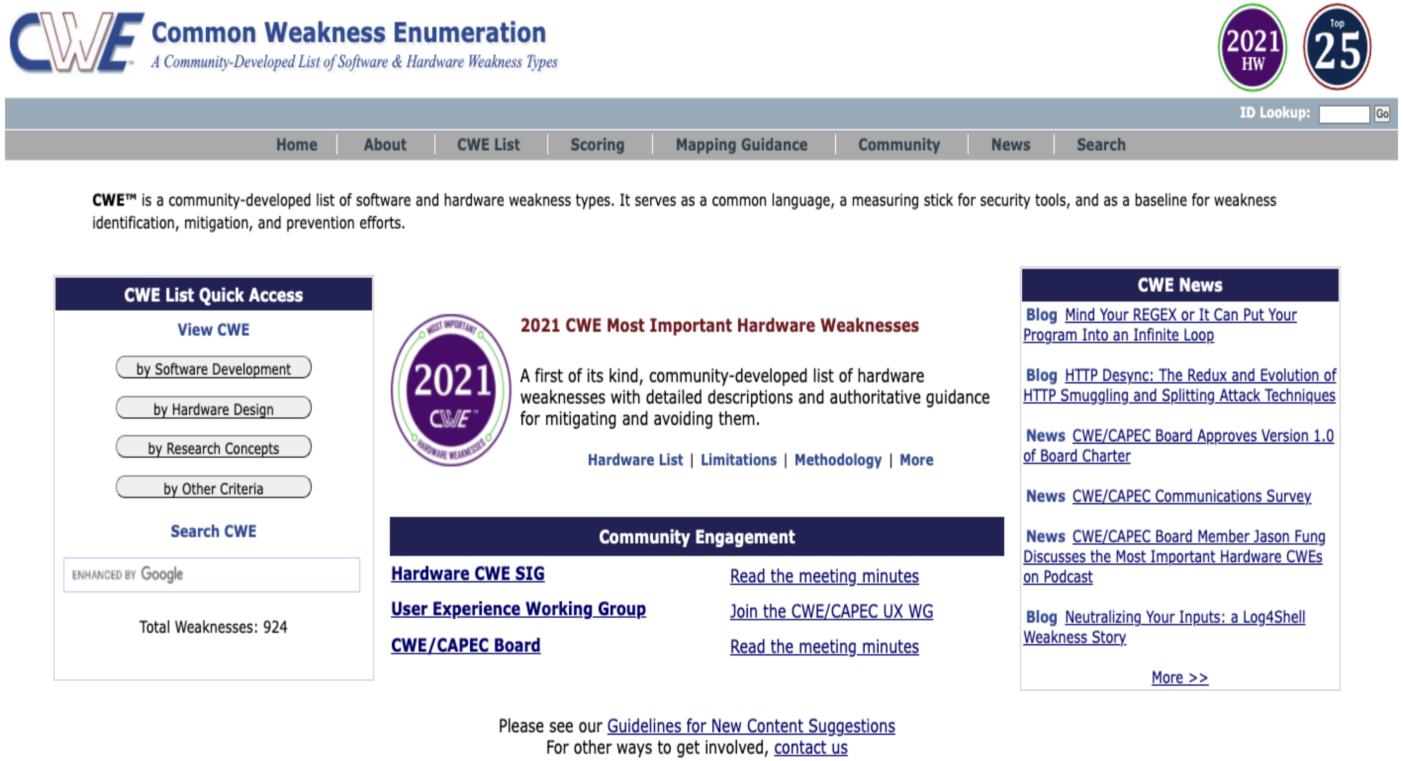
~1300 XSS Injection vulnerabilities in specific technologies in 2021

# 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.



**CWE™** is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

Total Weaknesses: 924

**2021 CWE Most Important Hardware Weaknesses**

A first of its kind, community-developed list of hardware weaknesses with detailed descriptions and authoritative guidance for mitigating and avoiding them.

| | |
|---|---|
| Hardware CWE SIG | Read the meeting minutes |
| User Experience Working Group | Join the CWE/CAPEC UX WG |
| CWE/CAPEC Board | Read the meeting minutes |

**Blog** Mind Your REGEX or It Can Put Your Program Into an Infinite Loop

**Blog** HTTP Desync: The Redux and Evolution of HTTP Smuggling and Splitting Attack Techniques

**News** CWE/CAPEC Board Approves Version 1.0 of Board Charter

**News** CWE/CAPEC Communications Survey

**News** CWE/CAPEC Board Member Jason Fung Discusses the Most Important Hardware CWEs on Podcast

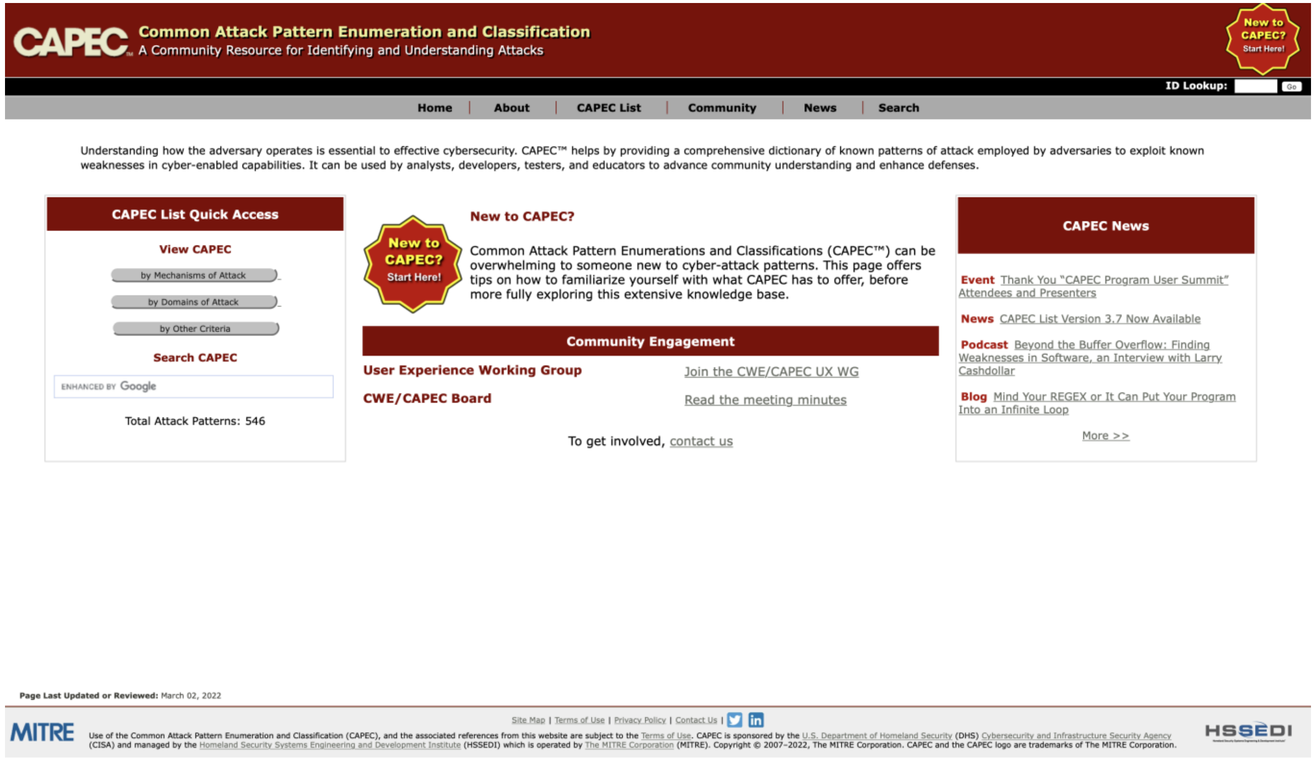
**Blog** Neutralizing Your Inputs: a Log4Shell Weakness Story

Please see our Guidelines for New Content Suggestions
For other ways to get involved, contact us

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

# 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)**



CAPEC™
New to CAPEC? Start Here!
ID Lookup:
Go
Home | About | CAPEC List | Community | News | Search

**Common Attack Pattern Enumeration and Classification**
A Community Resource for Identifying and Understanding Attacks

Understanding how the adversary operates is essential to effective cybersecurity. CAPEC™ helps by providing a comprehensive dictionary of known patterns of attack employed by adversaries to exploit known weaknesses in cyber-enabled capabilities. It can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses.

**CAPEC List Quick Access**

**View CAPEC**

by Mechanisms of Attack

by Domains of Attack

by Other Criteria

**Search CAPEC**

ENHANCED BY Google

Total Attack Patterns: 546

**New to CAPEC?**

Common Attack Pattern Enumerations and Classifications (CAPEC™) can be overwhelming to someone new to cyber-attack patterns. This page offers tips on how to familiarize yourself with what CAPEC has to offer, before more fully exploring this extensive knowledge base.

**Community Engagement**

**User Experience Working Group** Join the CWE/CAPEC UX WG

**CWE/CAPEC Board** Read the meeting minutes

To get involved, contact us

**CAPEC News**

**Event** Thank You "CAPEC Program User Summit" Attendees and Presenters

**News** CAPEC List Version 3.7 Now Available

**Podcast** Beyond the Buffer Overflow: Finding Weaknesses in Software, an Interview with Larry Cashdollar

**Blog** Mind Your REGEX or It Can Put Your Program Into an Infinite Loop

More >>

**Page Last Updated or Reviewed:** March 02, 2022

Site Map | Terms of Use | Privacy Policy | Contact Us |

MITRE

Use of the Common Attack Pattern Enumeration and Classification (CAPEC), and the associated references from this website are subject to the Terms of Use. CAPEC is sponsored by the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and managed by the Homeland Security Systems Engineering and Development Institute (HSSEDI) which is operated by The MITRE Corporation (MITRE). Copyright © 2007–2022, The MITRE Corporation. CAPEC and the CAPEC logo are trademarks of The MITRE Corporation.

HSSEDI

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).

# 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**