Agenda for the Cybersecurity Industry Advisory Board (CIAB) Meeting

November 23, 2021 at 2 PM

1. Approval of the minutes of the last board meeting held on 04/16/2021.
2. Brief review of updates to the IUP Cybersecurity Programs:
   - BS. in CompSci – Cybersecurity Track
   - Minor in Cybersecurity
   - COSC Courses
3. Updates regarding the status of our CAE PoS and designation applications.
4. Continue the discussion of the following topics:

   a) Considering the removal of the requirement of the Minor in Criminology

   b) Updating the requirements to better fit the CAE revised 2020 Knowledge Units (KUs) Framework, see next page.

   c) Including modules focusing on scripting, offensive security, vulnerability assessments, cyber leadership, etc. in the Cybersecurity curriculum

   d) Providing recommendation of possible ways to implement CIAB recommendations with the current limited resources.
5. Deciding on the spring 2022 meeting date.
6. Questions/final comments.

APPENDIX 1 – REQUIRED AND OPTIONAL KNOWLEDGE UNITS LIST FOR CAE-CD

(3) Foundational (all required): IT Systems Components (ISC), Cybersecurity Foundations (CSF), and Cybersecurity Principles (CSP)

(5) Core KUs required of all PoS. Individual programs choose to align to Technical or Non-Technical Core KUs depending on the nature of their PoS. Associates and Bachelors programs are required to align courses in the PoS to the Technical or Non-Technical KUs. Graduate programs may either align to these KUs, or may provide detailed documentation on how the institution verifies that students have met these KUs. For example, the institution may document a system in place that allows for checking of prior courses and/or other experiences of entering graduate students to demonstrate the Foundational and Core KUs or require them to take courses and/or other experiences to achieve the Foundational and/or Core KUs lacking before entering or during the program.

The five technical **core** KUs are:

- Basic Scripting and Programming (BSP)
- Basic Networking (BNW)
- Network Defense (NDF)
- Basic Cryptography (BCY)
- Operating Systems Concepts (OSC)

The five non-technical **core** KUs are:

- Cyber Threats (CTH)
- Policy, Legal, Ethics and Compliance (PLE)
- Security Program Management (SPM)
- Security Risk Analysis (SRA)
- Cybersecurity Planning and Management (CPM)

Optional KUs (56 total) can be adopted by any program as needed to document their program of study. Additionally, opposing core KUs may be used as optional KUs (i.e. If technical core is chosen, then non-technical core may be used as optional KUs and if non-technical core is chosen, then technical core maybe used as optional KUs.). Optional KUs include:

Advanced Algorithms (AAL)	**Fraud Prevention and Management (FPM)**	**Operating Systems Theory (OST)**
Advanced Cryptography (ACR)	**Hardware Reverse Engineering (HRE)**	**Operating System Administration (OSA)**
Advanced Network Technology and Protocols (ANT)	**Hardware/Firmware Security (HFS)**	**Penetration Testing (PTT)**
Algorithms (ALG)	**Host Forensics (HOF)**	**Privacy (PRI)**
Analog Telecommunications (ATC)	**IA Architecture (IAA)**	**QA/Functional Testing (QAT)**
Basic Cyber Operations (BCO)	**IA Compliance (IAC)**	**Radio Frequency Principles (RFP)**
Cloud Computing (CCO)	**IA Standards (IAS)**	**Secure Programming Practices (SPP)**
Cyber Crime (CCR)	**Independent/Directed Study/Research (Emerging Topics) (IDR)**	**Software Assurance (SAS)**
Cybersecurity Ethics (CSE)	**Industrial Control Systems (ICS)**	**Software Reverse Engineering (SRE)**
Data Administration (DBA)	**Introduction to Theory of Computation (ITC)**	**Software Security Analysis (SSA)**
Data Structures (DST)	**Intrusion Detection/Prevention Systems (IDS)**	**Supply Chain Security (SCS)**
Database Management Systems (DMS)	**Life-Cycle Security (LCS)**	**Systems Certification and Accreditation (SCA)**
Databases (DAT)	**Low Level Programming (LLP)**	**Systems Programming (SPG)**
Device Forensics (DVF)	**Media Forensics (MEF)**	**Systems Security Engineering (SSE)**
Digital Communications (DCO)	**Mobile Technologies (MOT)**	**Virtualization Technologies (VVT)**
Digital Forensics (DFS)	**Network Forensics (NWF)**	**Vulnerability Analysis (VLA)**
Embedded Systems (EBS)	**Network Security Administration (NSA)**	**Web Application Security (WAS)**
Forensics Accounting (FAC)	**Network Technology and Protocols (NTP)**	**Wireless Sensor Networks (WSN)**
Formal Methods (FMD)	**Operating Systems Hardening (OSH)**	

https://www.iad.gov/nietp/Requirements.cfm