The Challenge of Building the Cyber Workforce

- Technology innovation is ramping up to address growing cybersecurity threats
- Critical challenges remain to address the need to develop a capable cyber workforce to maintain both national security and economic interests
- Private sector, government and educational institutions need to work together to help inspire our next generation of innovators and cyber operators
- The high cost of training and organizing and retaining a capable cyber force is the single greatest challenge to governments

BLUF: This workshop address strategies, challenges and opportunities in developing, nurturing and growing a national cyber workforce
Considerations when Building the Cyber Workforce

- In order to meet the dire requirements for a cyber workforce, governments must take a holistic approach to developing a workforce.

- Courses must build upon each other and allow individuals to enter curriculum streams based on their present skill from beginner to expert, utilizing competency exams.

- Curriculum must have a heavy emphasis on hands-on practical application so students can move into filling cyber security positions.

- Consideration of building and operating a cyber range to support hands-on training is critical.

- Training should be mapped to independent standards that are transferable across organizations in the public and private realm.
Logistic Considerations

- **Program Management**

- **Student Enrollment considerations**
  - Identify and recruit students
  - Identify students capable of receiving security clearance
  - To comply with applicable national laws & regulations
  - Standard language proficiency
  - Psychological tests to ensure greater success

- **Facility Maintenance**
  - Partner shall be responsible for maintaining thin clients and other hardware and equipment in each classroom. This may include software patches, firewall upgrades, etc.
Key Training Considerations

- Curriculum designed around mission-critical environments and scenarios
- Offense and defense are integrated and operational
- Classroom, instructor-led web-module, and on-demand
- Cyber Range for practical applications
Cyber Curriculum

Pipeline for Building the Cyber Workforce

Curriculum supports the NIST and NICE Framework (National Initiative for Cyberspace Education) certifications
Cyber Range Considerations

Complete Range Tool Set For Exercises and Vulnerability Assessments

**Critical Infrastructure**

**Plan ➔ Deploy ➔ Execute ➔ Recover**

Cyber Range Data Center
Provides Virtualized Infrastructure and Layer 1 Switching

System Under Test

**Blue Team**
Provides Network Defense Services to Defend Against Cyber Penetration

**White Team**
Provides Rules of Engagement, Game Referee, and Test Monitoring and Control Services

**Red Team**
Provides Network Penetration Services

**Range Operations**
Provides Range Management and Configuration Control Services

**Visualization Center**
Provides Viewing Area of Event Testing and Supports After Action Review

**Training Center**
Provides Space for Basic Cyber Training and Real-World Scenario

Hardware in the Loop Environment (HWIL)
Provides space for customer hardware testing (OPTIONAL - see pare 3.4.5)
DESCRIPTION
This course provides the basic, foundational knowledge common across all cybersecurity work roles. The course could also serve as an entry level for those who are interested in seeking a career in cybersecurity but do not have the required experience or computer background.

TARGET AUDIENCE
Entry-level cyber operators
Intermediate Cyber Training

DESCRIPTION
This course provides deeper knowledge of network fundamentals, cyber vulnerabilities, Information Assurance (IA) standards and cybersecurity risk mitigation. The course includes a boot camp to focus on the key learning objectives for achieving industrial certifications (e.g., Network+).

TARGET AUDIENCE
Security and Network Operations Center (SOC/NOC) operators
General Cyber Operator Training

DESCRIPTION
This course builds specialized experts by teaching students the core skills needed for the different cyber disciplines and introduces them to the various cyber professional roles. This course is intended as a broad overview of the cyber disciplines. The course also includes a boot camp to focus on the key learning objectives for achieving industrial certifications (e.g., Security+).

TARGET AUDIENCE
Cyber generalists, service help desk personnel and technical supervisors who are interested in deepening their cyber knowledge without specialization in any particular discipline
Security Operations Center (SOC) Training

DESCRIPTION
This course builds core skills for specialized cyber positions. Security Operations Center (SOC) operators perform defensive tasks such as incident response, signature development and attack analysis. The course includes a boot camp to focus on the key learning objectives for achieving industrial certifications.

TARGET AUDIENCE
Security and Network Operations Center (SOC/NOC) operators
DESCRIPTION
This course builds core skills for specialized cyber positions. Forensics analysts perform defensive tasks such as collecting and analyzing open-source information for incident investigations. The course includes a boot camp to focus on the key learning objectives for achieving industrial certifications.

TARGET AUDIENCE
Forensics analysts, cyber analysts and malware analysts
Penetration Tester Training

DESCRIPTION
This course builds core skills for specialized cyber positions. Penetration testers perform defensive tasks such as open-source collection and analysis, threat intelligence and vulnerability analysis. The course includes a boot camp to focus on the key learning objectives for achieving industrial certifications (e.g., Certified Ethical Hacker [CEH]).

TARGET AUDIENCE
Penetration testers and threat intelligence analysts
DESCRIPTION
This course builds specialized experts by teaching students the core skills needed for the different cyber disciplines and introducing them to the roles cyber professionals perform. Malware analysts perform defensive tasks such as open-source collection and analysis, secure malware handling and reporting, and performing static analysis and reverse engineering. The course includes a boot camp to focus on the key learning objectives for achieving industrial certifications.

TARGET AUDIENCE
Forensics analysts and cyber analysts
Advanced Technical Lead Training

DESCRIPTION
This course provides advanced knowledge and practical application for the cyber workforce across all cyber disciplines. It also builds leadership skills for the cyber workforce. Practical exercises are integrated throughout the curriculum to ensure students learn by doing and the course culminates in a capstone/lab exercise. The course also includes a boot camp to focus on the key learning objectives for achieving certification (e.g., CISSP).

TARGET AUDIENCE
Cyber team leaders who oversee a wide range of cyber operations and seek advanced knowledge across all cyber disciplines (i.e., penetration testing, SOC Operations, cyber analyst)
Executive Awareness Training

DESCRIPTION
This course is tailored for an executive audience and requires a basic awareness of cyber threats and how they impact the overall mission. This course is an overview of the threats and basic security measures leadership should take to protect their organization. This course provides an overview of the problem without getting into the technical details. No computer background is required for this course.

TARGET AUDIENCE
Executives, senior managers, leaders and organizational decision makers
DESCRIPTION
This course targets managers that lead cyber teams. These leaders require a broad understanding of the cyber threat, defensive capabilities and tools and the roles within a cyber team. This 30-hour course assumes students will be overseeing cyber operations, so they need to understand the problems and how they can be mitigated. This course outlines the major cyber roles and tools. A computer background is highly advised for this course.

TARGET AUDIENCE
Technical managers, team leaders and supervisors
Workforce Organization and Staffing

- Organizational Development
  - Cyber Defense organizational structures
  - Governance
  - Sourcing strategies
  - Industry and government partnerships

- Staffing
  - Job Definitions and Recruitment
  - Classroom and Self-Directed Training
  - On the Job Training
  - Leadership Development
  - Performance Assessment

- Awareness
  - Broad awareness programs
  - Compliance testing and promotion
Process Training

- Concept of Operations
- Standard Operating Procedures
- Risk Management
- Priority Information Requirements
- System Security Plans and Certification
- Executive Communication
- Incident Handling & Field Operations
- Forensics
- Situation Reporting
- Active Defense TTPs
- Tool Maintenance
- Agile Development
- Program Management
  - CRM, CMMI, Integrated Development, EVMS
- Secure Supply Chain Management
- Knowledge Capture and Transfer
Technology Training

- Facilities Construction
- Data Center Construction
- SIEM Deployment
- Sensors and Collectors, Logging & Audit
- Cross Domain Information Sharing
- Identity Systems & Management
- End Point Security
- System Hardening
- Network Zoning, Firewalls, IPS
- Gateway & Proxies
- Insider Threat Monitoring
- Vulnerability & Penetration Testing
- Threat Intelligence Feeds
- Open Source Collection
- Analytics, Predictive & Behavioral
- Hunter & Fly-Away Kits
- Help Desk
- Governance, Risk & Compliance
- Forensics, Malware Reverse Engineering
Questions and Comments