ACRONYMS

ACL - Access Control Lists
AES - Advanced Encryption Standard
ASI - Authorized Service Interruption
BGP - Border Gateway Protocol
CIA - Confidentiality, Integrity, Availability
COOP - Continuity of Operations Plan
DLP - Data Loss Prevention
DNS - Domain Name Server
HBSS - Host Based Security System
IAM - Identity Access Management
IDS - Intrusion Detection System
IPS - Intrusion Prevention System
JSON - JavaScript Object Notation
LDAP - Lightweight Directory Access Protocol
LUA - Lightweight Programming Language
NICE - National Initiative for Cybersecurity Education
NIST - National Institute of Standards and Technology
OSI - Open Systems Interconnection
PCAP - File format for Packet Capture
PCI - Payment Card Industry
PHI - Protected Health Information
PI - Proprietary Information
PKI - Public Key Infrastructure
PMI - Preventive Maintenance Interruption
POAM - Plan of Actions & Milestones
RADIUS - Remote Authentication Dial-In Service
RFI - Request for Information
RMA - Risk Management Assessment
RMF - Risk Management Framework
SEIM - Security Event and Incident Management
SQL - Structured Query Language
STIG - Service Technical Implementation Guide
TACAS - Terminal Access Controller Access System
TCP - Transmission Control Protocol
VLAN - Virtual Local Area Network
VPN - Virtual Private Network
WPA - WiFi Protected Access

DACUM Panel

Dr. Gregory Braxton, Newport News Shipbuilding
Kane Crisler, Packet Forensics
Joshua Cox, Towne Bank
Eric Hacecky, Thomas Jefferson National Accelerator Facility
Colleen Lammers, Booz Allen Hamilton
Jim Newman, Peregrine
Richard Severinghaus, CRTN Solutions, LLC
Stephen Watkins, G2 Ops, Inc.
Major Dennis A. Adezas, Joint Forces Staff College
Jennifer Romero, CISSP, AERMOR, LLC

DACUM Facilitator

Jennifer Stevens, Chief Operating Officer
Virginia Advanced Study Strategies

Developed under a grant provided by the National Institute of Standards and Technology’s National Initiative for Cybersecurity Education.
<table>
<thead>
<tr>
<th><strong>Duties</strong></th>
<th><strong>A.01</strong></th>
<th><strong>A.02</strong></th>
<th><strong>A.03</strong></th>
<th><strong>A.04</strong></th>
<th><strong>A.05</strong></th>
<th><strong>A.06</strong></th>
<th><strong>A.07</strong></th>
<th><strong>A.08</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assess</strong></td>
<td>Identify info system assets</td>
<td>Identify security vulnerabilities</td>
<td>Identify attack vectors</td>
<td>Quantity business value of assets</td>
<td>Brief stakeholders *</td>
<td>Review policies and procedures</td>
<td>Test response processes</td>
<td>Create virtual test environments</td>
</tr>
<tr>
<td><strong>Cyber</strong></td>
<td><strong>Risks</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Tasks</strong></th>
<th><strong>B.01</strong></th>
<th><strong>B.02</strong></th>
<th><strong>B.03</strong></th>
<th><strong>B.04</strong></th>
<th><strong>B.05</strong></th>
<th><strong>B.06</strong></th>
<th><strong>B.07</strong></th>
<th><strong>B.08</strong></th>
<th><strong>B.09</strong></th>
<th><strong>B.10</strong></th>
<th><strong>B.11</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protect</strong></td>
<td>Create protection plan</td>
<td>Create contingency plan</td>
<td>Create disaster recovery plan</td>
<td>Provision user accounts</td>
<td>Implement access controls (i.e. black lists, white lists, geofence)</td>
<td>Install network devices (i.e. IDS, IPS, firewalls, web filters)</td>
<td>Configure network devices (i.e. IDS, IPS, firewalls, web filters)</td>
<td>Install host-based security systems (i.e. anti-viruses, malware, sensors)</td>
<td>Configure host-based security systems (i.e. anti-viruses, malware, sensors)</td>
<td>Create investigative and configuration scripts</td>
<td>Ensure data encryption (i.e. data at rest, data in transit removable media)</td>
</tr>
<tr>
<td><strong>Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Assets</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Protect</strong></th>
<th><strong>B.12</strong></th>
<th><strong>B.13</strong></th>
<th><strong>B.14</strong></th>
<th><strong>B.15</strong></th>
<th><strong>B.16</strong></th>
<th><strong>B.17</strong></th>
<th><strong>B.18</strong></th>
<th><strong>B.19</strong></th>
<th><strong>B.20</strong></th>
<th><strong>B.21</strong></th>
<th><strong>B.22</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protect</strong></td>
<td>Ensure physical security controls</td>
<td>Ensure environmental controls</td>
<td>Recommend security requirements</td>
<td>Manage wireless access points</td>
<td>Create network diagrams</td>
<td>Maintain network diagrams</td>
<td>Create penetration test plans</td>
<td>Request ASI</td>
<td>Backup critical data</td>
<td>Manage network device life-cycles</td>
<td></td>
</tr>
<tr>
<td><strong>Information</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Assets</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Detect</strong></th>
<th><strong>C.01</strong></th>
<th><strong>C.02</strong></th>
<th><strong>C.03</strong></th>
<th><strong>C.04</strong></th>
<th><strong>C.05</strong></th>
<th><strong>C.06</strong></th>
<th><strong>C.07</strong></th>
<th><strong>C.08</strong></th>
<th><strong>C.09</strong></th>
<th><strong>C.10</strong></th>
<th><strong>C.11</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cyber</strong></td>
<td>Monitor network devices</td>
<td>Analyze output of network devices</td>
<td>Analyze threat feeds</td>
<td>Monitor wireless access points</td>
<td>Review network diagrams</td>
<td>Set audit flags</td>
<td>Analyze external data (i.e. darknet, passive DNS, BGP)</td>
<td>Document historical findings</td>
<td>Maintain historical Packet Capture (PCAP)</td>
<td>Analyze audit logs</td>
<td>Analyze vulnerability scans</td>
</tr>
<tr>
<td><strong>security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Events</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Detect** | **C.12** | **C.13** | **C.14** | **C.15** | | | |
|-----------|----------|----------|----------|----------|-------|
| **Cyber** | Hunt potential threats in network traffic | Conduct organizational penetration tests | Generate penetration test documentation | Challenge personnel need-to-know/authorization | |
| **security** | | | | | |
| **Events** | | | | | |

<table>
<thead>
<tr>
<th><strong>React</strong></th>
<th><strong>D.01</strong></th>
<th><strong>D.02</strong></th>
<th><strong>D.03</strong></th>
<th><strong>D.04</strong></th>
<th><strong>D.05</strong></th>
<th><strong>D.06</strong></th>
<th><strong>D.07</strong></th>
<th><strong>D.08</strong></th>
<th><strong>D.09</strong></th>
<th><strong>D.10</strong></th>
<th><strong>D.11</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>to</strong></td>
<td>Initiate response procedures</td>
<td>Assess security event</td>
<td>Report event to supervisor *</td>
<td>Determine escalation</td>
<td>Communicate with stakeholders *</td>
<td>Maintain stakeholder call list</td>
<td>Contain security incident</td>
<td>Trace source of threat</td>
<td>Preserve evidence of event</td>
<td>Document steps taken</td>
<td>Estimate damage of security incident</td>
</tr>
<tr>
<td><strong>Cyber</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Events</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **React** | **D.12** | **D.13** | **D.14** | | | | |
|-----------|----------|----------|----------|-------|
| **to** | Server network activity | Report estimated time of restoration | Document evidentiary process | |
| **Cyber** | | | | |
| **security** | | | | |
| **Events** | | | | |

<table>
<thead>
<tr>
<th><strong>G.01</strong></th>
<th><strong>E.01</strong></th>
<th><strong>E.02</strong></th>
<th><strong>E.03</strong></th>
<th><strong>E.04</strong></th>
<th><strong>E.05</strong></th>
<th><strong>E.06</strong></th>
<th><strong>E.07</strong></th>
<th><strong>E.08</strong></th>
<th><strong>E.09</strong></th>
<th><strong>E.10</strong></th>
<th><strong>E.11</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>E.01</strong></td>
<td>Determine scope of restoration</td>
<td>Create restoration plan</td>
<td>Coordinate restoration efforts</td>
<td>Rebuild info system</td>
<td>Reimage information system</td>
<td>Restore critical data</td>
<td>Test restored environment</td>
<td>Validate restored environment</td>
<td>Document lessons learned</td>
<td>Document recovery processes</td>
<td></td>
</tr>
<tr>
<td><strong>Restore</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Secure</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Environment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **F.01** | **F.02** | **F.03** | **F.04** | **F.05** | **F.06** | **F.07** | **F.08** | **F.09** | **F.10** | | |
|-----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|-------|
| **Increase** | Create security awareness materials | Create acceptable use policies | Participate in security exercises | Distribute security info to users | Conduct cybersecurity training | Conduct phishing campaign | Reverse engineer malware | Conduct security awareness assessment | Report assessment results | Recommend procedures to correct security issues | |
| **Security** | | | | | | | | | | | |
| **Awareness** | | | | | | | | | | | |

| **G.01** | **G.02** | **G.03** | **G.04** | **G.05** | **G.06** | **G.07** | | |
|-----------|----------|----------|----------|----------|----------|----------|-------|
| **Maintain** | Complete cybersecurity training | Maintain industry certifications | Read technical literature [i.e. books, blogs, articles, etc.] | Attend professional conferences | Maintain operating environment qualifications | Practice through trial and error | Maintain professional memberships | |
| **Professional** | | | | | | | |
| **Knowledge** | | | | | | | |

* Denotes a recurring task
Worker Behaviors

- Able to problem solve
- Able to work autonomously
- Able to work independently
- Self-starter
- Attention to detail
- Methodical
- Strong work ethic
- Integrity
- Oral/written communication skills
- Tenacious
- Team player
- Teachable
- Passionate about field
- Self-motivated
- Inquisitive
- Ethical
- Desire to learn
- Professionalism
- Common sense
- Conflict resolution
- Desire to work beyond minimum expectations
- Willing to be on call after hours
- Discretion
- Multi-tasker
- Creative

Knowledge & Skills

- Server management
- Load balancing
- UNIX
- SQL
- Linux
- OSI model
- Oracle
- Cisco
- TACACS +
- NoSQL
- Switches
- LDAP
- Common application ports
- Routers
- Kerveros
- TCP/IP
- Snort
- RADIUS
- Volatility
- Wire shark/T shark
- X TACACS
- SPLUNK
- Nessus
- Rainbow Tables
- Maltego
- Endpoint protection software
- Visualization tools
- SEIM tools
- Scapy
- Common application protocols
- Cloud environments
- Raspberry pi
- Node JS
- Regulation policies
- LUA
- “Google-fu”
- GIT
- NIST
- APIs
- JavaScript
- JSON
- Programming languages
- Tenacity
- LUA
- DISCERN
- NIST
- LUZ
- API
- SSH
- LUA
- JSON
- APIs
- Parsing
- Endpoint protection software
- Parsing
- LUA
- Open source intelligence
- NIST
- Python
- Powershell
- LUA
- NIST
- Python
- C Programming
- LUA
- RESTful APIs
- LUA
- Assembly Programming
- LUA
- RESTful Interfaces
- LUA

Tools, Equipment, Supplies, and Materials

- Visio (MS)
- FTP Voyager
- Packet analysis software
- Packet tracer
- Google
- GNS3
- Putty
- Virtual machines
- Printer
- Lab environment
- Laptop
- Through put tester
- Monitors
- Latency simulator
- Ethernet cable
- T-Bird
- USB cable
- Vision network icon
- Serial console cable
- Crimper
- Ethemet cable
- Wireless LAN tools
- Cable tester/TDR
- Site survey tools
- Multimeter
- WPA2
- File transfer client
- WEP
- Notepad ++
- PHP
- Scripting
- Apache
- YARA
- WPA2
- Encryption
- LUA
- WEP
- Packet sniffers
- LUA
- Linux
- 802.1x
- Open source intelligence
- Python
- Open source intelligence
- Firewalls
- LUA
- SSH/Serial Communications
- Encryption
- LUA
- PKE/PKI
- C Programming
- LUA
- Python
- Assembly Programming
- LUA

Recommendations for Recruiting Students

- Cybersecurity club
- Capture the flag events
- Create /use of a cyber-range to build, test, destroy, and restore
- College/university partner with companies - real data and scenarios needed for training
- Companies offer internships and opportunities for project-based learning
- Cyber Honors Program – computer science majors apply and do extra cyber work for rewards
- Scholarships (Cyber Corps)
- Offer course on security culture

Future Trends

- Cybersecurity jobs in high demand
- Trained individuals have ability to choose where they work
- Cybersecurity yields higher salary (vs. networking)
- Stigma of cybersecurity as a “boring” or “stuffy” field
- Public lacks understanding of the wide variety of cyber roles
- Concerns about industrial SCADA
- Internet of Things
- Cybercrime escalation - direct impact on lives
- Cyber espionage
- Cybercrime over software-defined radio