Current Cyber Landscape

This Overall Classification of this Briefing is:

UNCLASSIFIED//FOUO

Major Christopher Allen

Executive Direction

- **Presidential Policy Directive/PPD-21 – Critical Infrastructure Security and Resilience (12 Feb 2013)**
  - National unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure

- **Presidential Executive Order – Promoting Private Sector Cybersecurity Information Sharing (13 Feb 2015)**
  - Encouraging Private-Sector Cybersecurity Collaboration
  - Enabling Better Private-Public Information Sharing
  - Providing Strong Privacy and Civil Liberties Protections

- **Presidential Executive Order – Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber –Enabled Activities (1 April 2015)**
  - Authority to respond to the threat posed by malicious cyber actors

Legislative Direction

- **The Protecting Cyber Networks Act (H.R. 1560) - April 2015**
  - Voluntary Information Sharing between private companies and federal government (non-DoD and NSA)
  - Cyber Threat Indicators for Cybersecurity Purposes **ONLY**
  - Congressional Oversight

- **National Cybersecurity Protection Advancement Act (H.R. 1731) April 2015**
  - Department of Homeland Security's (DHS) center for integrating cyber threat information is the National Cybersecurity and Communications Integration Center (NCCIC)
    - Solely to prevent and respond to cyber attacks
    - Protect the privacy and civil liberties of all Americans
    - Pro-privacy, pro-security bill ensures the sharing of cyber threats is transparent and timely

Department of Defense Direction

- **DoD**
  - Defend DoD networks, systems, and information
  - Defend the United States and its interests against cyberattacks of significant consequence
  - Provide integrated cyber capabilities to support military operations and contingency plans

- **USCYBERCOMMAND (USCC)**
  - DoD Cyber professionals will grow by 6000+ by FY 18

- **United States Air Force (USAF)**
  - AFSPC/24AF/67CW/26COG/33NWS
  - ANGRC/102NWS
  - JTF Cyber

- **Rhode Island (JTF Cyber/DHS?)**
  - RI JFHQ/102NWS

102 NWS Mission

Citizen Airmen providing Active/Passive DCO & Intel capabilities to USCYBERCOM, USAF, DHS, FEMA Region I and RI to defend, deny, detect, analyze, research and report network intrusions and vulnerabilities.

USAF Requirements

- **Air Force Cyberspace Defense (ACD) Weapon System-Computer Network Defense Service Provider (CNDSP) for the AFIN**
  - 24/7/365 monitoring of AF cyber domain
    - Real-time response to and investigation of network/computer intrusions
    - CNDSP for 3rd party enclaves
      - COCOM
      - AOC
      - USAF/Joint R&D

- **Pro-active Defense and Defensive Counter Cyber – Pursuit (DCC-P)**

Rhode Island Cyber Disruption Team (RI CDT)

- **Primary Role of ANG as member of RI Cyber Disruption Team**

  - **Participate in Bi-Monthly meetings since 2012**

  - **Summer 2014 participated in HOT SIM training with RI State Police**

  - **Sponsor/Mentor for Cyber Patriot**

  - **Multiple RI EMA cyber Tabletops**

  - **Cyber Yankee 2015**

  - **Limited to Train, Advise, Assist (TAA) Role**

    - **Legal Limitations**

    - **SAD Requirements – Direct EMA/CDT coordination**

Military Capabilities

- **Cyberspace Operations Planning Team**
  - Integrates Cyberspace Ops in the Order of Battle

- **Defensive Cyberspace Operations Crew**
  - Detect/defend/deny adversary freedom of action in an AOR
  - Supports Critical Infrastructure
  - Analyzes/secures/creates affects to establish/maintain superiority
  - Defends friendly info against adversary efforts
  - Coordinated/integrates with air/space/cyberspace to enhance ops

- **Cyberspace Intelligence**
  - Information Collaboration/Sharing
  - Preparation of Operational Environment
  - Battle Damage Assessment

Cyber Skills Civilian Snapshot

- ## DSG Civilian Positions

  - **Information Security Analyst**
  - **Information Technology Manager**
  - **Network Engineer**
  - **Systems Engineer**
  - **Computer Support Analyst**
  - **Infrastructure Technician**
  - **Technical Systems Analyst**

- ## Degrees

  - **Communications**
  - **Information Systems**
  - **Cyber Security**
  - **Information Assurance**

- ## Certifications

  - **BIST**
  - **CCNA**
  - **CEH**
  - **CISSP**
  - **DISA Level 1**
  - **GCIH/GSEC**
  - **Security+**

Emergency Support Functions (ESF)

- **1) Effects Delivery – These ESFs perform functions resulting in the direct delivery of life saving or property protection effects.**
    - **1. ESF #3 – Public Works and Engineering**
    - **2. ESF #4 – Firefighting (air and ground)**
    - **3. ESF #6 – Mass Care, Emergency Assistance, Temporary Housing, and Human Services**
    - **4. ESF #8 – Public Health and Medical Services**
    - **5. ESF #9 – Search and Rescue**
    - **6. ESF #10 – Oil and Hazardous Materials Response**
    - **7. ESF #13 – Public Safety and Security**

- **2) Enablers – These ESFs perform functions primarily in support of two or more of the Effects Delivery ESFs, enabling them to deliver lifesaving or property protection effects.**
    - **1. ESF #1 – Transportation (air and ground)**
    - **2. ESF #2 – Communications**
    - **3. ESF #5 – Information and Planning (includes Emergency Management and Incident**

Limiting Factors

- **Title and Authority (Legal)**

  - **State Active Duty**

  - **Title 32**

  - **Title 10**

- **Equipment Utilization**

  - **RI-EMA/RI CDT procured RAPID-TAC equip (previous slides)**

  - **Currently cannot utilize Federal Air Force Cyberspace Defense (ACD) Weapon System assets on critical infrastructure, OGA or civilian networks**

  - **ANG to field VITE NLT FY17 for 10 National Cyber Units 102 NWS)**

Critical Infrastructure

- **Academia, Civilian/Business, OGA, State Government, Utilities**

- **Focus on interoperability, Training, Info Sharing**

  - Academia – MIT LL, Hanscom AFB

  - Medical - Blue Cross Blue Shield RI, CVS Health

  - Financial – Citizen's Bank

  - Insurance – FM Global, Amica

  - Industrial/Utilities – National Grid

  - Intellectual Property/PII – All, Dell

  - Government – DHS, DIA, State of RI, NE Region

Questions?