# CYBER INFRASTRUCTURE PROTECTION WORK GROUP

Paul Kurtz

# Work Update

- Joint CSOC Proposal
  - An identified need for better coordination between Federal, state, local, and private sector entities
- State Agency Cyber Survey
  - Concerns with length of survey have delayed survey issuance
- Leveraging National Guard assessment assets for use in localities
- Targeted meetings with other states
  - Michigan Cyber Security Initiative
  - Oklahoma Cyber Command
- Targeted meetings with state agencies
  - Virginia Army National Guard
  - Virginia State Police - Fusion Center
  - Virginia Information Technology Agency

# Joint CSOC Proposal

- Cyber Security Operations Center Mission
  - To provide public and private sector participants with a common operating picture by administering a collaborative environment in which participating organizations can better coordinate and share information and resources.
    - Live monitoring of participant systems
      - Threat Information Sharing
      - Incident Response
      - Recovery Operations
      - Mutual Aid

# Participation

- Public and Private Sector Participants
  - State – Governor's Office, VITA, VANG, VSP
  - Federal – FBI
  - Local
  - Private Sector

# Next Steps

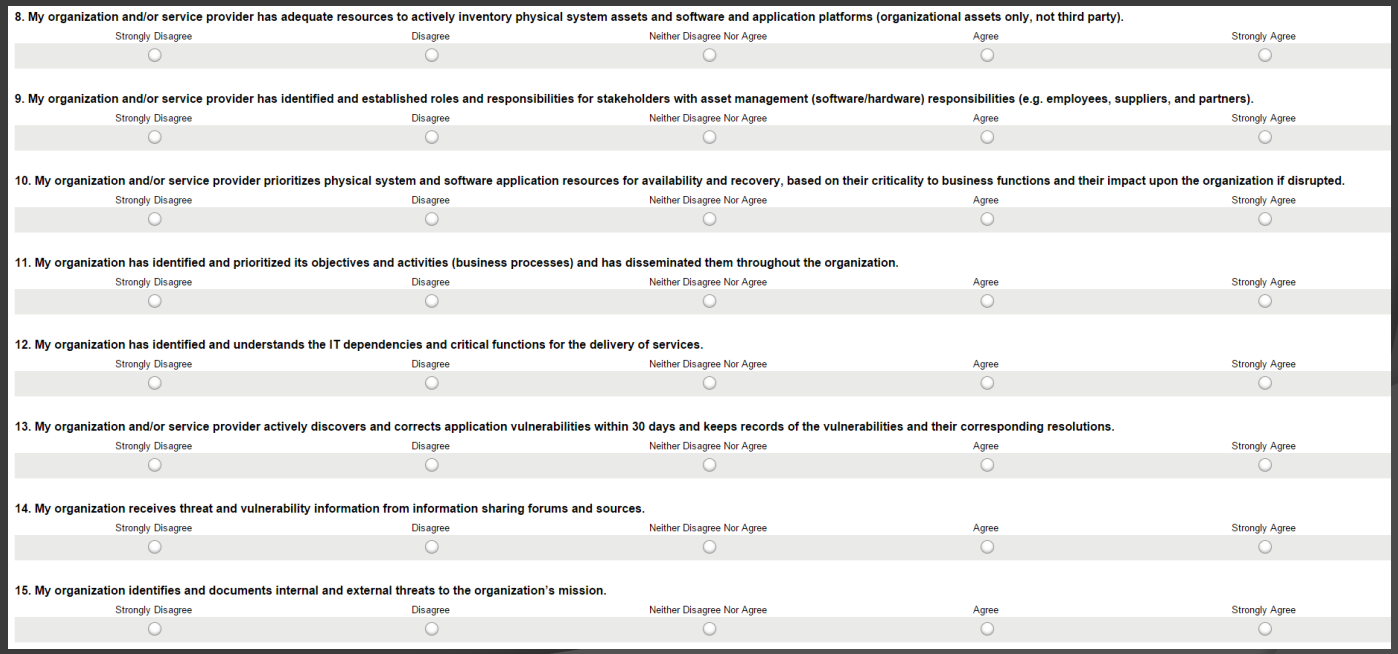
- IOC Review
  - Review issues requiring further elaboration
    - Leadership and Staffing
    - Source feeds and analytical tools
    - Enabling technologies
    - Finance and costs
    - Incentives for participant organizations
  - 14 day review period
- Draft budget item for submission by November 21

# State Agency Survey

- Review of existing capabilities, programs, and initiatives
  - Get an understanding of the current operating picture and what improvements/changes need to be made
- Considerations to the impact on agency ISOs
  - The survey has been designed to maximize response
  - Estimated time to take survey is 15 - 30 minutes

# State Agency Survey

- Survey state agencies on cyber security
  - Executive, legislative, and judicial
  - NIST Cyber Framework Core Functions
    - Identify, Protect, Detect, Respond, Recover
  - Will be composed of 56 self assessment questions
    - Multiple Choice



**8. My organization and/or service provider has adequate resources to actively inventory physical system assets and software and application platforms (organizational assets only, not third party).**

| Strongly Disagree | Disagree | Neither Disagree Nor Agree | Agree | Strongly Agree |
|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ |

**9. My organization and/or service provider has identified and established roles and responsibilities for stakeholders with asset management (software/hardware) responsibilities (e.g. employees, suppliers, and partners).**

| Strongly Disagree | Disagree | Neither Disagree Nor Agree | Agree | Strongly Agree |
|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ |

**10. My organization and/or service provider prioritizes physical system and software application resources for availability and recovery, based on their criticality to business functions and their impact upon the organization if disrupted.**

| Strongly Disagree | Disagree | Neither Disagree Nor Agree | Agree | Strongly Agree |
|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ |

**11. My organization has identified and prioritized its objectives and activities (business processes) and has disseminated them throughout the organization.**

| Strongly Disagree | Disagree | Neither Disagree Nor Agree | Agree | Strongly Agree |
|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ |

**12. My organization has identified and understands the IT dependencies and critical functions for the delivery of services.**

| Strongly Disagree | Disagree | Neither Disagree Nor Agree | Agree | Strongly Agree |
|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ |

**13. My organization and/or service provider actively discovers and corrects application vulnerabilities within 30 days and keeps records of the vulnerabilities and their corresponding resolutions.**

| Strongly Disagree | Disagree | Neither Disagree Nor Agree | Agree | Strongly Agree |
|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ |

**14. My organization receives threat and vulnerability information from information sharing forums and sources.**

| Strongly Disagree | Disagree | Neither Disagree Nor Agree | Agree | Strongly Agree |
|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ |

**15. My organization identifies and documents internal and external threats to the organization's mission.**

| Strongly Disagree | Disagree | Neither Disagree Nor Agree | Agree | Strongly Agree |
|---|---|---|---|---|
| ○ | ○ | ○ | ○ | ○ |

# Next Steps

- Survey
  - Deliver survey to state agencies
  - Analyze survey responses
    - Colleges and Universities

# National Guard Assessment Capability

- Reviewing how VANG can assist localities in conducting vulnerability assessments of their information systems
  - Development of an approved CONPLAN in no less than 90 days
  - Questions of the frequency of assessments, funding, etc. must be addressed

# Execution Timeline

- November
  - Seek approval for survey issuance
  - Draft letter on behalf of Commission and engage agencies via Webinar
  - Issue survey
- November 21
  - Have a detailed proposal with budget prepared for the Joint CSOC
- Mid-December
  - Receive survey responses
  - Engage with college and university partners for analysis of survey results
- Jan – Feb
  - Develop CONPLAN of VANG assessment capability for localities

# Questions?