Virginia State Police Briefing

Brian J. Moran
Secretary of Public Safety
& Homeland Security

Senate Finance Committee Meeting
June 15, 2017

Agenda

- Background: Status of Network & Incident
- Response Effort: Unified Command & Actions Taken
- Path Forward
- Core Mission Not Impacted

Background: Status of VSP Network

VSP Out of Scope Network	VSP In-Scope Network
• Accounts for roughly 80% of the network	• Accounts for about 20% of network
• Includes an estimated 300 servers to support VSP mission	• Includes email exchange and active directory as well as end user systems (Desktops/Laptops)
• Includes 2,070 Mobile Computer Terminals in Trooper vehicles and support to 450 law enforcement agencies across the Commonwealth	• Considered in-scope to VITA but non-transformed

Background: VSP Malware Incident

- Occurred on April 21, 2017
- Malware downloaded as a result of a link embedded in a phishing email
- Malware got ahold of VSP active directory and spread across in-scope network
- As a mitigating action, VSP disconnected from email and Internet to prevent further compromise

Response Effort: Actions Taken

- VITA/NG, working with VSP, scanned each computer/server at SPHQ and in the Field
  - Status as of June 8th:
    - SPHQ – 81 computers require reimaging (to remove malware infection)
    - Field – 49 computers require reimaging
- MS-ISAC contacted for third-party review of infection
- Containment of malware is only a temporary solution; complete rebuild of network is necessary to bring VSP back to full operations
- Email access has been restored to VSP workstations
- Working with VITA/NG to restore full web access
- Daily reporting from VSP and VITA

Response Effort: Unified Command

- Given criticality of agency mission, the Governor's Office established a Unified Command to oversee response process and make recommendations on a path forward
  - Unified Command composed of National Guard and VDOT staff
  - Primary incident handlers are VSP and VITA
- Unified Command met directly with VSP and VITA to gather information and make recommendations on response process and path forward

Path Forward

- Containment of known malware is nearly complete
- Decision making process is underway to determine path forward for infrastructure rebuild based on recommendations by VSP, VITA, and Unified Command
  - New infrastructure must be in compliance with SEC501 (VITA's security standard)
- Engaging third party IT security firm to perform security analysis and make recommendations on security implementations
  - Will work with VSP, VITA, and the Unified Command

Questions?