Agenda

• VSP Network Breakdown
• Incident & Actions Taken
• Current Status
• Security and Infrastructure Review
• Path Forward
• Core Mission Not Impacted
# VSP Network Makeup

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

• Occurred on April 21, 2017
• Malware downloaded as a result of a link embedded in a phishing email
• VSP disconnected from email and Internet to prevent further compromise
• Each computer/server at SPHQ and in the Field scanned
• Given criticality of agency mission, the Governor’s Office established a Unified Command
• MS-ISAC conducted third-party review of infection
Current Status

- Containment of malware is only a temporary solution; complete rebuild of network is necessary to bring VSP back to full operations
- Email and restricted Internet access has been restored to VSP workstations
- Working with VITA/NG to scan/clean 183 remaining workstations – total cost of $115,692
- Daily reporting from VSP
Security and Infrastructure Review

• Timeline
  – Kickoff: Monday, September 18th
  – Concurrent on-site security infrastructure review
  – Completion: 8 weeks (November)

• Deliverables:
  – Findings from comprehensive review of infrastructure and security program
  – Recommendation on infrastructure rebuild and security implementation (transformation vs. separation)
Path Forward

- Containment of known malware is complete
- Establish interim solutions to support VSP operations until rebuild occurs
- Work with third party firm to ensure the most comprehensive analysis possible
- Conduct rebuild of VSP network to meet Commonwealth security standards
Questions?