Office of CyberSecurity
Response Capabilities

David Morris
CTO CyberSecurity
Relationships

- **MS-ISAC**
  - Information Sharing, Education, Training

- **US-CERT**
  - Cyber Incident Analysis, Forensics

- **NCCIC**
  - Monitoring, Alerting of Malicious Cyber Activity

- **Office of Cyber Security, State of Washington**
  - State Government
  - Local Government
  - Political Subdivisions
  - Critical Infrastructure
  - Tribal Government
Building Trust

- Security is all about building trust relationships
- These relationships need to be in place before they are needed
### Partnership Benefits

**Government advantage of information sharing**

<table>
<thead>
<tr>
<th>Solutions</th>
<th>Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personnel</td>
<td>Systems</td>
</tr>
<tr>
<td>• Awareness materials</td>
<td>• Threat Intelligence</td>
</tr>
<tr>
<td>• Training</td>
<td>• Common Operational Picture</td>
</tr>
<tr>
<td>• Shared Knowledge</td>
<td></td>
</tr>
</tbody>
</table>
Framework

- Computer Emergency Readiness Team (CERT)
  - Continuous Monitoring
  - Event Correlation
  - Packet Analysis

- Security Operations Center (SOC)
  - Mitigation
  - Forensics
  - Incident Handling
Computer Emergency Readiness Team (CERT)

CERT personnel fill a role analogous to that of a firefighter.

<table>
<thead>
<tr>
<th>Assessment</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive review</td>
<td>Remote Deployment</td>
</tr>
<tr>
<td>Risk Identification</td>
<td>Coordinated with Agency Resources</td>
</tr>
<tr>
<td>Objective</td>
<td>Certified Experts</td>
</tr>
<tr>
<td>Custom modules</td>
<td>Forensics Expertise</td>
</tr>
</tbody>
</table>
Computer Emergency Readiness Team (CERT) Assessment Example
Computer Emergency Readiness Team (CERT)

Response Example: Fish and Wildlife

- Petty criminal cyber actor: “MrHigh”
- Self reported
- Multiple states impacted: WA, OR, ID
  - WA: 2,435,452 records (Last 4 of SSN #)
OCS Operational Picture

Week of January 15 – January 21

Security Operations Center
• 26 Alerts
  • Malicious Software (17)
  • Investigations (5)
  • Account Compromise (4)

Response Team
• 2 Response Incidents

Digital Forensics
• 2 Cases
Summary

• Security is empowered by relationships
• The Office of Cyber Security maintains two operational groups for detection and alerting
• The Computer Emergency Readiness Team responds to significant security incidents for State of Washington agencies, boards, and commissions
• The State of Washington is considered a leader amongst its peers

Questions?