IDAHO CYBERSECURITY

Jeff Weak
Administrator
Information Technology Services
AGENDA

- State IT Initiatives
- Cybersecurity
- Incident Response Program
STATE IT INITIATIVES – IT MODERNIZATION

• Vision
  • Unify IT for the state under a single organization
  • Agencies focus on their core business, not IT
  • Standardized, enterprise solutions

• Current Phase (multi-year initiative)
  • Eight agencies
  • ITS will double in size – 66 FTE
  • Expanded Services
    • Service Desk, Server/Storage Maintenance, Network, Cybersecurity (SOC and CISO office), Compliance, Phones, Application Development
CYBERSECURITY INITIATIVES

- NIST Cybersecurity Framework & NIST 800-53
- CIS Controls
- Vulnerability assessments/penetration tests
- **Annual cybersecurity awareness training**
  - Address #1 threat: human factor
- State cybersecurity website: https://cybersecurity.idaho.gov/
**INCIDENT RESPONSE PROGRAM**

**NOT IF, BUT WHEN...**

- Vision: a future in which various government entities in our great state work together to prepare and respond to cybersecurity incidents

- ITS, Emergency Management, Department of Homeland Security, counties, municipalities

- Built around the NIST SP 800-53
  - Governance
INCIDENT RESPONSE PROGRAM

- VERIS - Framework
  - Common language
  - Repeatable
  - Metrics / Analytics

- WebEOC – Collection
  - Common Platform
  - Accessible
  - Secure
## Incident Response Program

### Summary View

<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Source ID</th>
<th>Confidence Rating</th>
<th>Victim ID</th>
<th>Incident Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### New Record Button

#### Common Language based on VERIS
<table>
<thead>
<tr>
<th>Incident ID</th>
<th>Event Type</th>
<th>Position</th>
<th>Name</th>
<th>Phone</th>
<th>Date</th>
<th>Point of Contact</th>
<th>Address/Location</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Routine Status Report</td>
<td>ID Cybersecurity Coordination</td>
<td>Diego Curt</td>
<td>(208) 202-1891</td>
<td>4/13/2019 05:39:46</td>
<td>ID Cybersecurity Coordination</td>
<td>ID Cybersecurity Coordination</td>
<td>This is a NO REPLY email address WebEOC Login: <a href="https://webserver.idaho.gov/ecd">https://webserver.idaho.gov/ecd</a>?</td>
</tr>
<tr>
<td>2</td>
<td>Routine Status Report</td>
<td>ID Cybersecurity Coordination</td>
<td>Kmil Umatit</td>
<td>208-356-4511</td>
<td>3/23/2019 19:49:44</td>
<td>ID Cybersecurity Coordination</td>
<td>ID Cybersecurity Coordination</td>
<td>This is a NO REPLY email address WebEOC Login: <a href="https://webserver.idaho.gov/ecd">https://webserver.idaho.gov/ecd</a>?</td>
</tr>
<tr>
<td>3</td>
<td>Routine Status Report</td>
<td>ID Cybersecurity Coordination</td>
<td>Diego Curt</td>
<td>(208) 356-4511</td>
<td>3/27/2019 14:11:16</td>
<td>ID Cybersecurity Coordination</td>
<td>ID Cybersecurity Coordination</td>
<td>This is a NO REPLY email address WebEOC Login: <a href="https://webserver.idaho.gov/ecd">https://webserver.idaho.gov/ecd</a>?</td>
</tr>
</tbody>
</table>

Event log for collaboration (Blue team assistance, agency comms, etc.)
QUESTIONS