



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

WebEOC | diego.curt | ID Cybersecurity Coordination | ID Cybersecurity | Log Out

1. Cybersecurity Event Log | 2. Cybersecurity Reporting

Cybersecurity Reporting

Search: Search Clear Search

[Export Report](#) [New Record](#)

Incident ID	Source ID	Confidence Rating	Victim ID	Incident Summary	Update Record
	test1sadf			afdsafdsasaf	<input type="button" value="Update Record"/> <input type="button" value="Details"/>

[Return to Beginning](#)

Summary View

New Record Button

Common Language based on VERIS

2. Cybersecurity Reporting Display - Internet Explorer

https://webservice.imd.idaho.gov/eoc7/boards/board.aspx?viewid=11444&tableid=2429&dataid=&relateddataid=0&uvid=1.63618.276874&hash=&filter=%7B%7D&mode

Remove Record Save

[Incident Tracking ?](#)

[Victim Demographics ?](#)

[Incident Description ?](#)

Actors: External

External: Motive

External: Variety

Actors: Internal

Internal: Motive Espionage Fear Financial Fun Grudge Ideology Convenience Unknown

Internal: Variety

Actors: Partners

Partner: Motive Espionage Fear Financial Fun Grudge Ideology Convenience Unknown

Partner: Variety

List View | Prev | Next

[Actions ?](#)

[Assets ?](#)

©2019 ESI Acquisition, Inc. WebEOC JUVARE

Cybersecurity Coordination Event Log

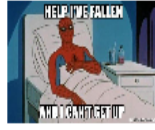
Incident: ID Cybersecurity [Event Log Report](#)

Record #: 8	Lance, and Faith, need to put together a rollout plan for after May 30th. Plan should include:	Event log for collaboration (Blue team assistance, agency comms, etc.)
Event Type: Routine Status Report	1. Initial announcement and training	
Position: County ID List ID Cybersecurity Coordination	2. Ongoing training	
Name: Diego Curt	3. Technical and Incident contact information	
Phone: (208) 332-1851	4. A plan to send sensitive information outside of WebEOC.	
Date: 04/18/2019 08:38:46	ID Cybersecurity Coordination - diego.curt at 08:38:46 on 04/18/2019	
Point of Contact:	This is a NO REPLY email address WebEOC Login: https://webserver.imd.idaho.gov/eoc7	
Attachments:		
Map:		
Address/Location:	Routine	Update Record Tasked Notes

This information is not for public disclosure and is intended for authorized WebEOC users only.

Record #: 7	I'm at the bottom of the building...Spiderman has died.	
Event Type: Routine Status Report	ID Cybersecurity Coordination - kdehart at 10:45:44 on 03/28/2019	
Position: County ID List ID Cybersecurity Coordination	This is a NO REPLY email address	
Name: Karl DeHart	WebEOC Login: https://webserver.imd.idaho.gov/eoc7	
Phone: 208-258-6531		
Date: 03/28/2019 10:45:44		
Point of Contact:		
Attachments:		
Map:		
Address/Location:	Routine	Update Record Tasked Notes

This information is not for public disclosure and is intended for authorized WebEOC users only.

Record #: 5	I am going to keep sending out a call for help for Spiderman until someone answers! Can someone answer this or is this a one-way notification?	
Event Type: Routine Status Report	ID Cybersecurity Coordination - diego.curt at 10:42:32 on 03/28/2019	
Position: County ID List ID Cybersecurity Coordination	This is a NO REPLY email address	
Name: Diego Curt	WebEOC Login: https://webserver.imd.idaho.gov/eoc7	
Phone: (208) 332-1851	Test, this is only a test: Spiderman has fallen and he can't get up.	
Date: 03/27/2019 14:11:16	ID Cybersecurity Coordination - diego.curt at 14:11:16 on 03/27/2019	
Point of Contact: Diego Curt	This is a NO REPLY email address	
Attachments:	WebEOC Login: https://webserver.imd.idaho.gov/eoc7	
Map: Spiderman Home		
Address/Location: 50 W. State Street, Boise, ID 83702	Routine	Update Record Tasked Notes

This information is not for public disclosure and is intended for authorized WebEOC users only.

QUESTIONS