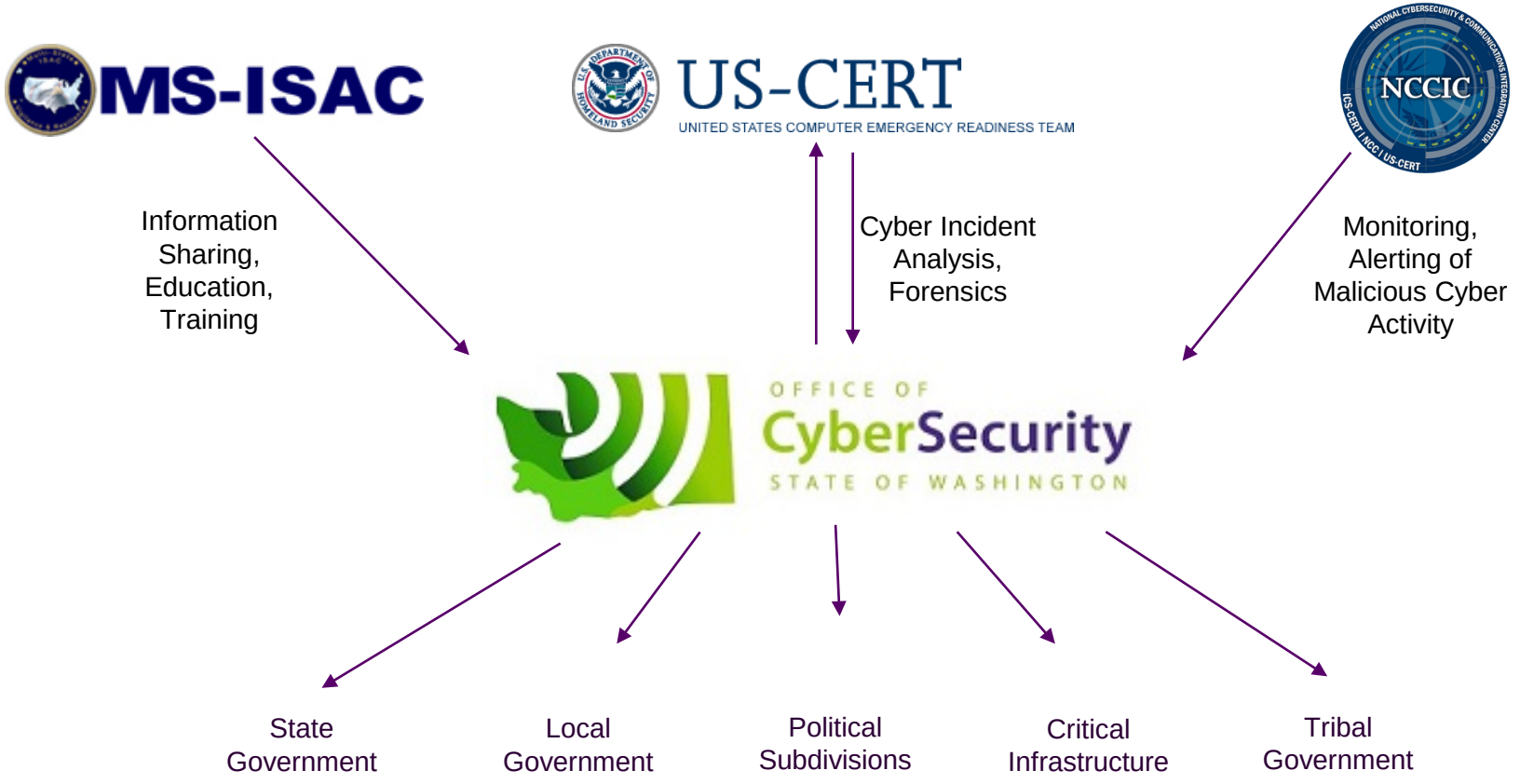
OFFICE OF
CyberSecurity
STATE OF WASHINGTON

Office of CyberSecurity Response Capabilities

David Morris
CTO CyberSecurity

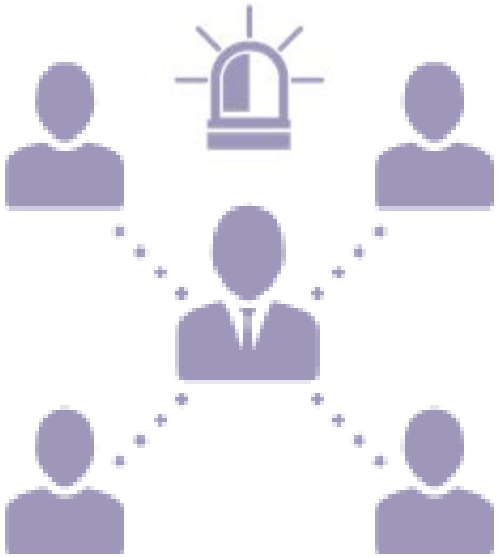
Relationships



OFFICE OF CyberSecurity STATE OF WASHINGTON

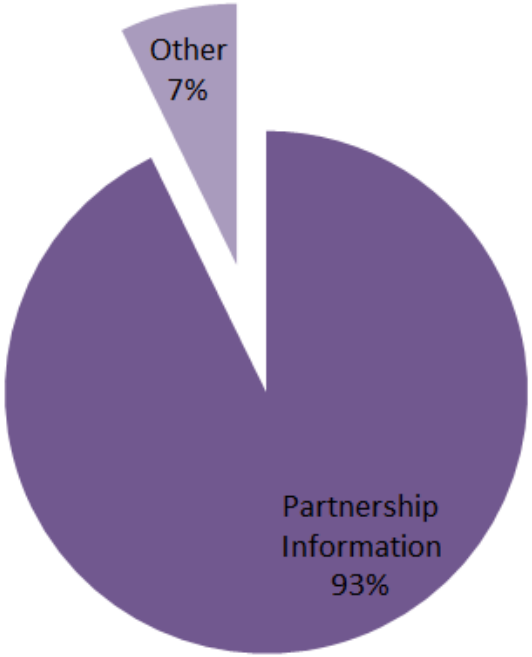
Building Trust

- 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



Categories

Solutions

Personnel	Systems	Services
• Awareness materials • Training • Shared Knowledge	• Threat Intelligence • Common Operational Picture	• Network Monitoring • Malware Analysis • Digital Forensics

Framework

- **Security Operations Center (SOC)**
  - Continuous Monitoring
  - Event Correlation
  - Packet Analysis
- **Computer Emergency Readiness Team (CERT)**
  - Mitigation
  - Forensics
  - Incident Handling

Computer Emergency Readiness Team (CERT)

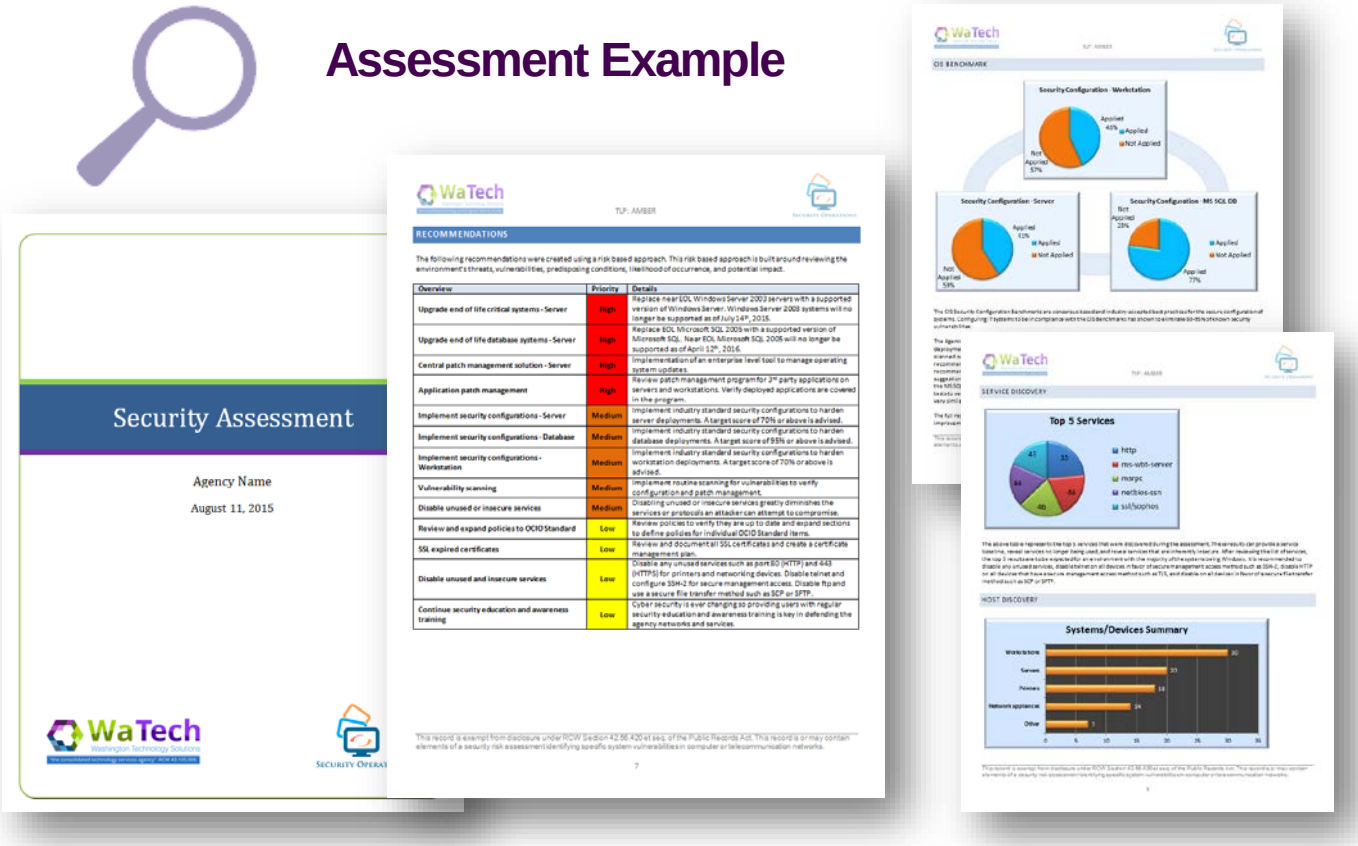
CERT personnel fill a role analogous to that of a firefighter

 **Assessment**	 **Response**
Proactive review Risk Identification Objective Custom modules	Remote Deployment Coordinated with Agency Resources Certified Experts Forensics Expertise

OFFICE OF CyberSecurity STATE OF WASHINGTON

Computer Emergency Readiness Team (CERT)

Assessment Example

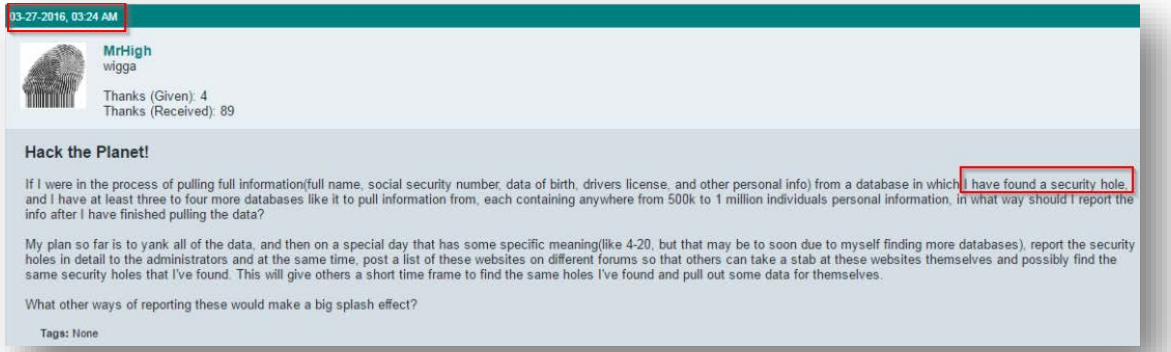


OFFICE OF CyberSecurity
STATE OF WASHINGTON

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 #)



OFFICE OF CyberSecurity STATE OF WASHINGTON

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

OFFICE OF CyberSecurity STATE OF WASHINGTON

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?