



# Alaska Department of Health and Social Services

Senate Health and Social Services  
DHSS Cyber Security Review  
February 8, 2022

Sylvan Robb, Assistant Commissioner  
Scott McCutcheon, HSS Department Technology Officer



# DHSS Cyberattack Timeline

- May 5: State Security Office detected malicious activity in a small number of DHSS systems and accounts
  - Impacted systems and accounts taken offline
  - Incident reported to law enforcement
- May 10: DHSS retained FireEye, a leading cybersecurity firm that provides incident response consulting services through Mandiant
- May 11: DHSS IT began advanced detection and analysis and shut off additional internal devices that had Indications of Compromise (IOC)
- May 17: All impacted systems were offline to prevent further disruption and harm to servers, systems, and data
- May 18: Public notified of the attack and disruption of services via social media and a press release

# Scope of the Cyberattack

- 19 systems were placed offline including:
  - DHSS Background Check System
  - Alaska Vital Records System
  - Alaska Behavioral Health and Substance Abuse Management System (AKAIMS)
  - DHSS Grants Electronic Management System (GEMS)
- Department Security Office determined that a possible data breach under the Health Insurance Portability and Accountability Act (HIPAA) had occurred
- DHSS notified Alaskans, offering credit monitoring for any Alaskan who requested the service

# Cyberattack Response Phases

- Detection and analysis
- Containment, eradication and recovery
- Post-incident activity

# DHSS Path Forward

- DHSS has restored nine systems to date including those mentioned:  
Background Check, Vital Records, AKAIMS, GEMS
- DHSS has ten systems in various phases of restoration using a 23-step build process
- DHSS is working with DOA OIT to enhance overall security posture and lower cyber risk
- DHSS proposes performing a Security Program Assessment that will provide recommendations to lower DHSS cyber risk