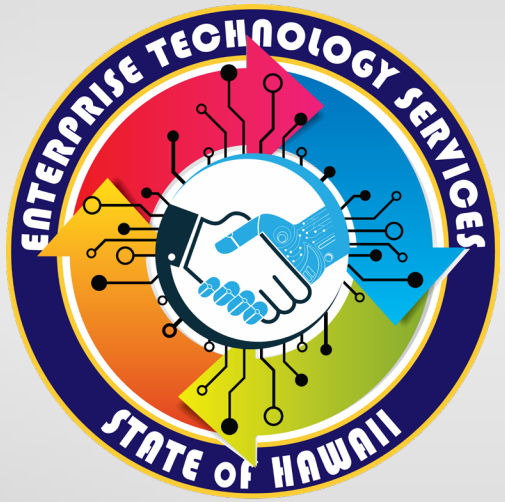
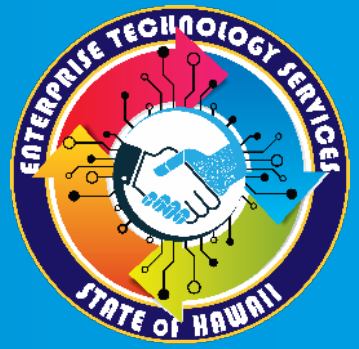


Untitled Goose Presentation

A State Cybersecurity Briefing

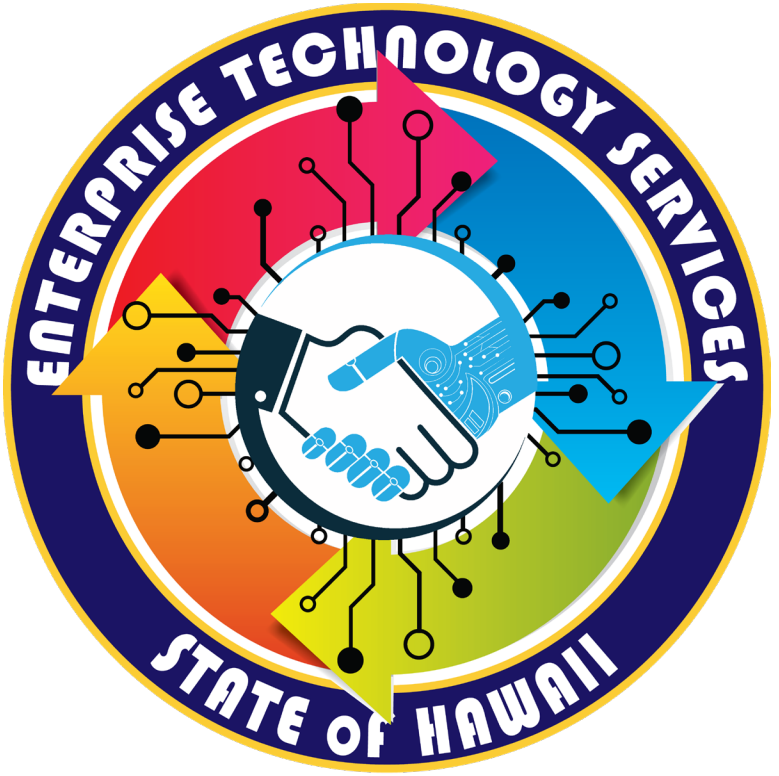
WED 05 APR 2023

Introduction



Introduction

- /usr/bin/whoami
  - Vince Hoang
  - Chief Information Security Officer



Introduction – About ETS

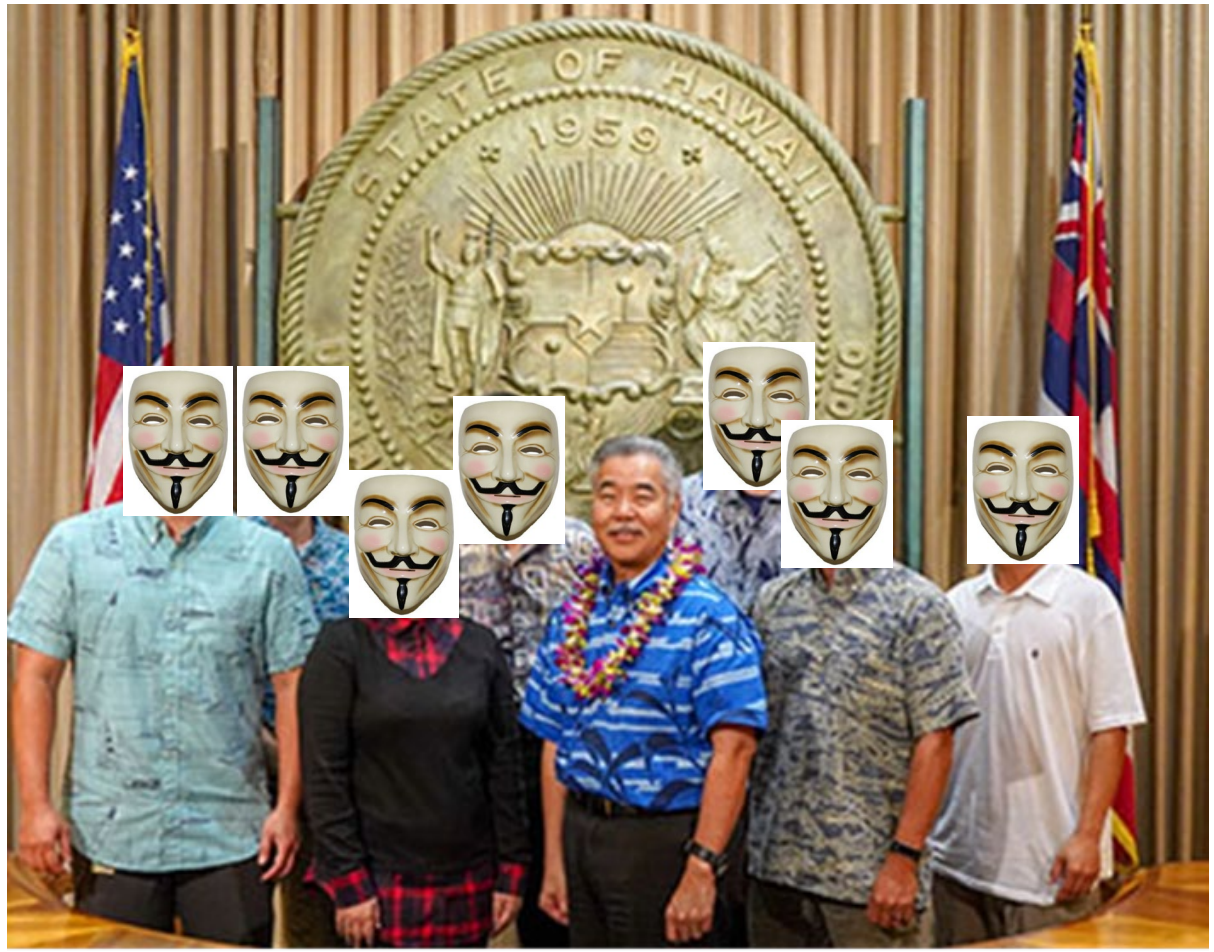
- /usr/bin/whatis ETS
  - Office of Enterprise Technology Services

Authority - Cybersecurity Related Statutes

HRS	Description
HRS §27-43	Act 58 of 2016 authorizes the CIO to coordinate each executive branch department and agency's IT budget request to ensure compliance … with ETS' IT governance processes and enterprise architecture policies and standards, including policies and standards for systems, services, hardware, software, and security management.
HRS §27-43.5	Provide for periodic security audits of all executive branch departments and agencies regarding the protection of government information and data communication infrastructure.
HRS §27-44	Set policies, procedures and standards for each executive branch department's reasonable efforts to make appropriate and existing electronic data sets maintained by the department electronically available to the public through the State's open data portal at data.hawaii.gov or successor website.
HRS §27G	Provide services through centralized web portal and Internet presence (hawaii.gov) that allow citizens to conduct business electronically with the government, in accordance with statute (i.e., Access Hawai'i Committee).
HRS §487N	Provide guidance to protect personal information that is collected and maintained by state and county government agencies (i.e., Information Privacy and Security Council).

https://www.capitol.hawaii.gov/hrsall/

Enterprise Technology Services Cyber Security Team



- Protects all branches of government that today share a common access point to the Internet — where most cyber threats originate!
- Allows ETS to pursue cost-effective solutions for cybersecurity by providing additional training to State employees.

Teamwork

Communication and Collaboration with Mission Partners

State Department of Defense Mission Partners

Division	Function
Office of Homeland Security Hawaii State Fusion Center (HSFC)	Nexus for intelligence briefings and federally sponsored training
Hawaii National Guard Cyber Mission Assurance Team (HI CYBER)	Assess and mitigate cyber security impacts to critical infrastructure
Hawaii Emergency Management Agency (HIEMA)	Coordinating to develop an Emergency Support Function (ESF) or annex in all hazards response plan

Federal or Federally Affiliated Mission Partners

Organization	Function
MS-ISAC - Multi-State Information Sharing and Analysis Center	Designated by Department of Homeland Security as the coordinating entity for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial governments.
CISA - Cybersecurity and Infrastructure Security Agency	Operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience
FBI - Federal Bureau of Investigation	Lead federal agency for investigating cyber attacks and intrusions

MS-ISAC
Multi-State Information Sharing and Analysis Center

- Designated by Department of Homeland Security as the coordinating entity for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial governments.
- Real-time, 24x7 network monitoring, early cyber threat warnings/advisories, vulnerability identification, and mitigation & incident response.

CIS Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

DHS CISA
Cybersecurity and Infrastructure Security Agency

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

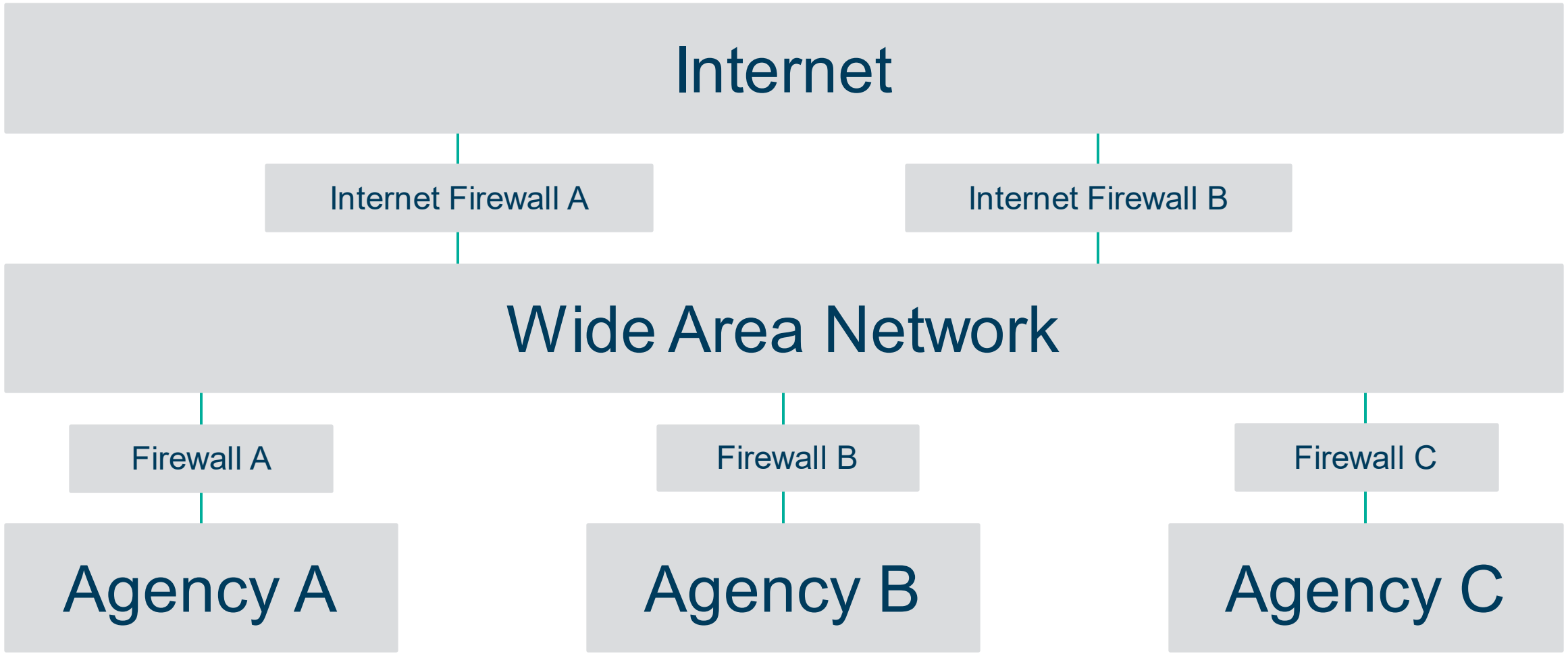
- External Vulnerability Scanning
  - Scans of departments and agencies external-facing public IP addresses
  - State of Hawaii has been a program participant since 2014 to help understand how sites appear to attackers on the Internet.
  - State departments and agencies review and take appropriate corrective action.
- Risk and Vulnerability Assessment
  - Remote web application assessment
  - Database security evaluations
  - On-site penetration test
- Joint Cyber Defense Collaborative
  - "The JCDC will bring together Federal, SLTT, and public-private stakeholders that possess relevant equities in cyber defense operations"

Embracing a Distributed Network and their Challenges

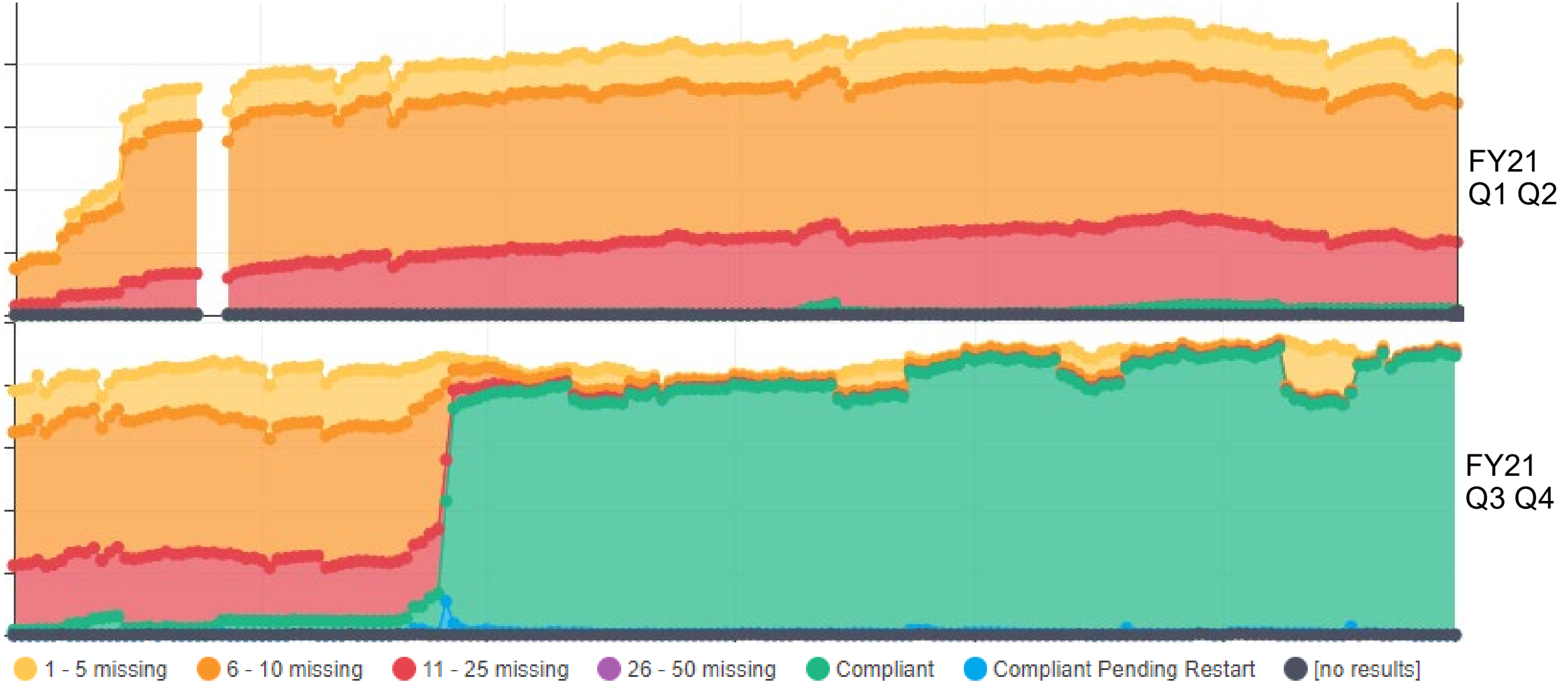
Shifting towards more Cloud Native Solutions

- Implemented Cloud Native Solutions
  - Microsoft Suite
    - Office 365
    - Azure Active Directory
    - Multi-Factor Authentication
    - Teams Calling
  - Electronic Signature
  - Endpoint Detection & Response
  - Emergency Notifications
  - Web Application Firewall / Content Delivery Network

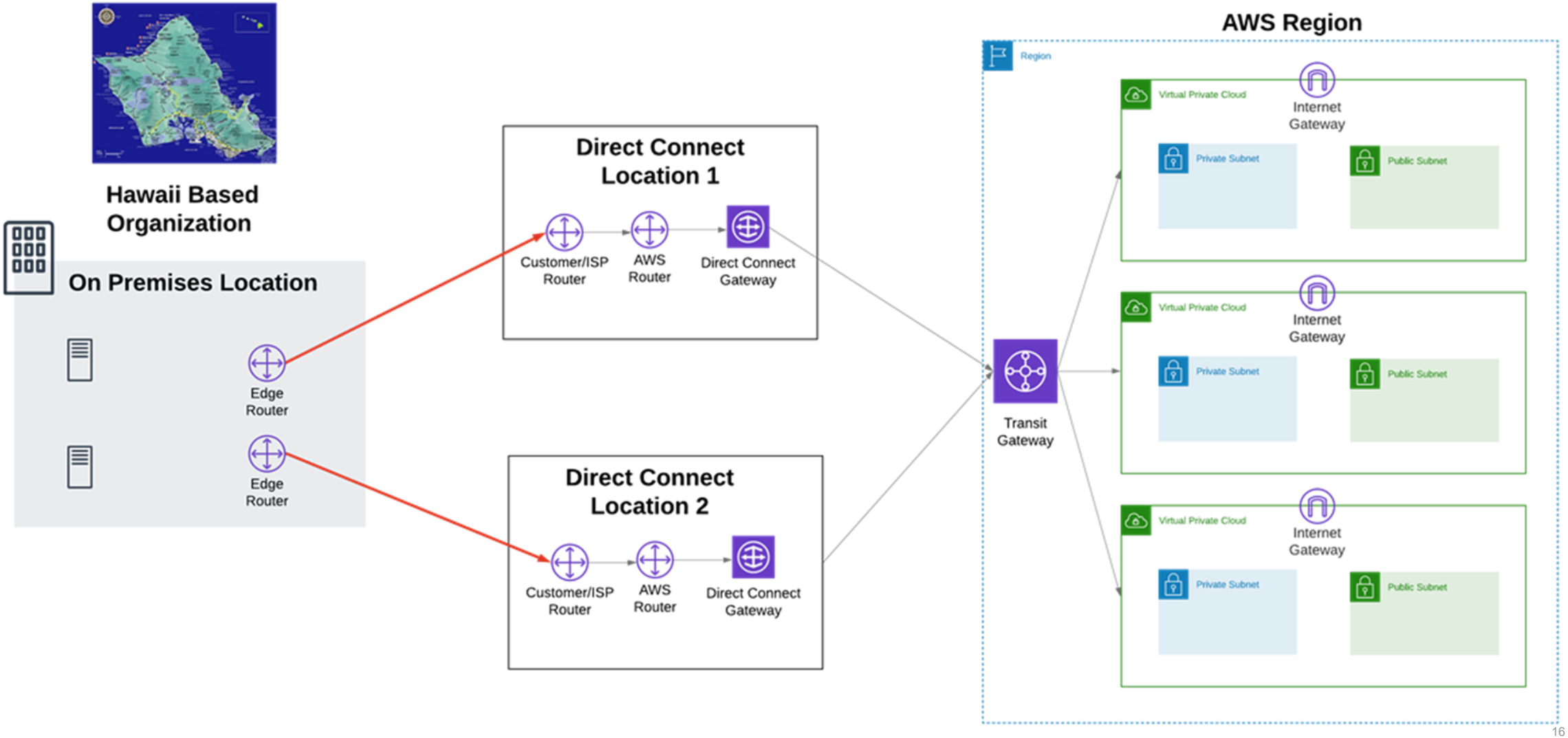
State Network



Agency B Windows Patch Status
Before and After “Patch-as-a-Service” Onboarding

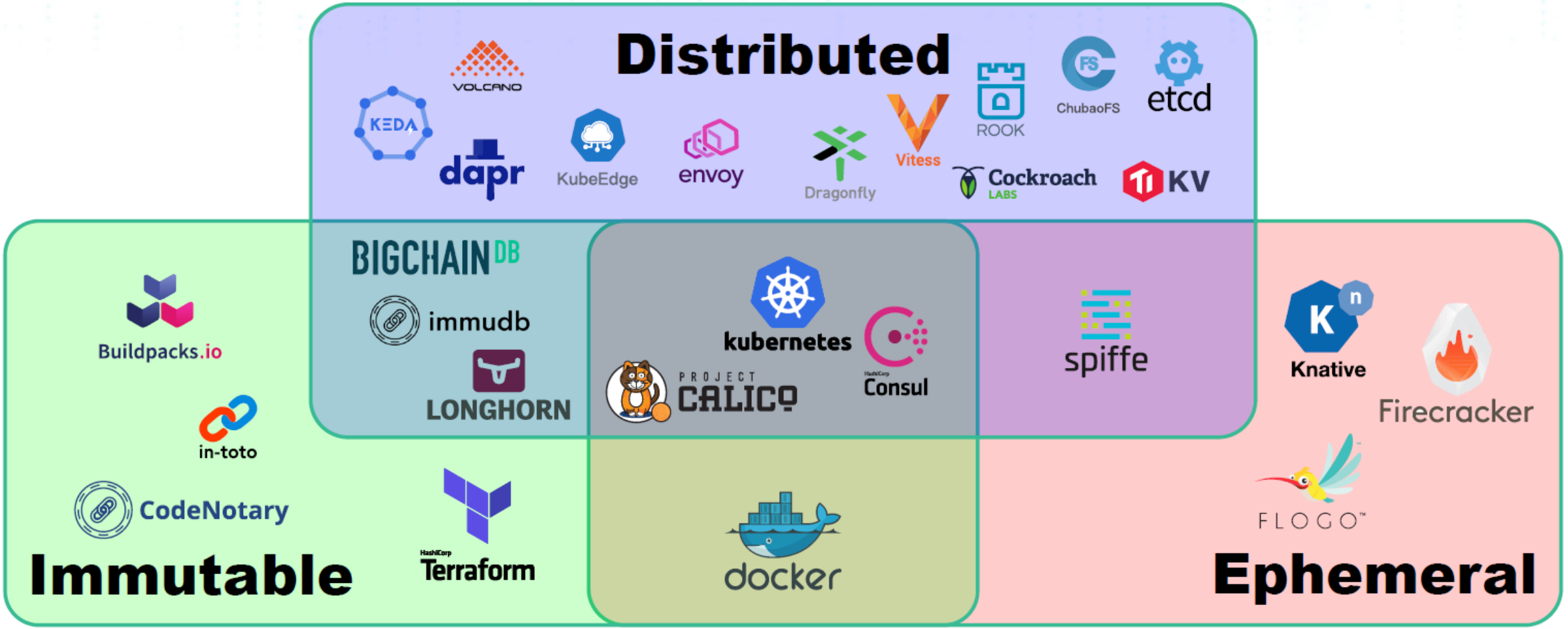


Problem – Limited Fiber



https://aws.amazon.com/blogs/architecture/building-resilient-and-high-performing-cloud-based-applications-in-hawaii/

DIE Triad



https://www.rsaconference.com/Library/presentation/USA/2021/death-to-cia-long-live-die-how-the-die-triad-helps-us-achieve-resiliency

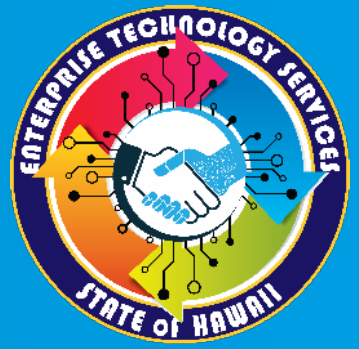
Untitled Goose Tool

A Hunt and Incident Response Tool for Use in Azure, Azure Active Directory, and Microsoft 365 Environments

- CISA advises network defenders to use Untitled Goose Tool to:
  - Export and review AAD sign-in and audit logs, M365 unified audit log (UAL), Azure activity logs, Microsoft Defender for IoT (internet of things) alerts, and Microsoft Defender for Endpoint (MDE) data for suspicious activity.
  - Query, export, and investigate AAD, M365, and Azure configurations.
- With this tool, network defenders can:
  - Extract cloud artifacts from Microsoft's AAD, Azure, and M365 environments without performing additional analytics.
  - Perform time bounding of the UAL via goosey graze.
  - Extract data within those time bounds with goosey honk.
  - Interrogate and collect data using similar time bounding capabilities for MDE data.

https://www.cisa.gov/sites/default/files/2023-03/untitled_goose_tool_fact_sheet_final_508cv2.pdf

Questions?



HRS §5-7.5 – Aloha Spirit

- "Akahai", meaning kindness to be expressed with tenderness;
- "Lokahi", meaning unity, to be expressed with harmony;
- "Oluolu", meaning agreeable, to be expressed with pleasantness;
- "Haahaa", meaning humility, to be expressed with modesty;
- "Ahonui", meaning patience, to be expressed with perseverance.

https://www.capitol.hawaii.gov/hrscurrent/Vol01_Ch0001-0042F/HRS0005/HRS_0005-0007_0005.htm