WIAF Forum 2017:
Cyber Security and IT Auditing
October 30, 2017

ETS
OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

Todd Nacapuy
Chief Information Officer
State of Hawaii

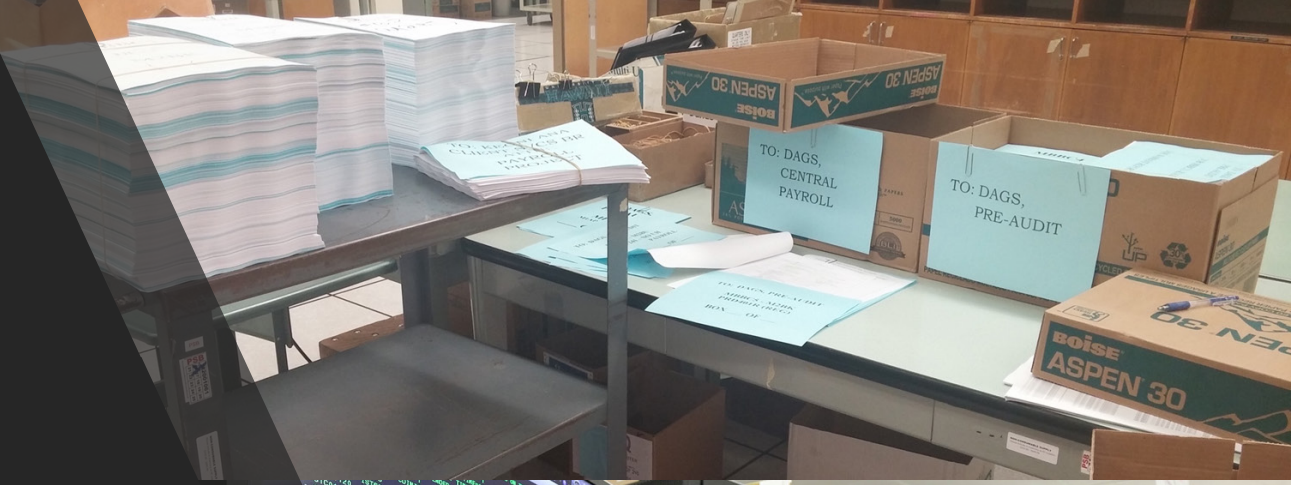
About ETS

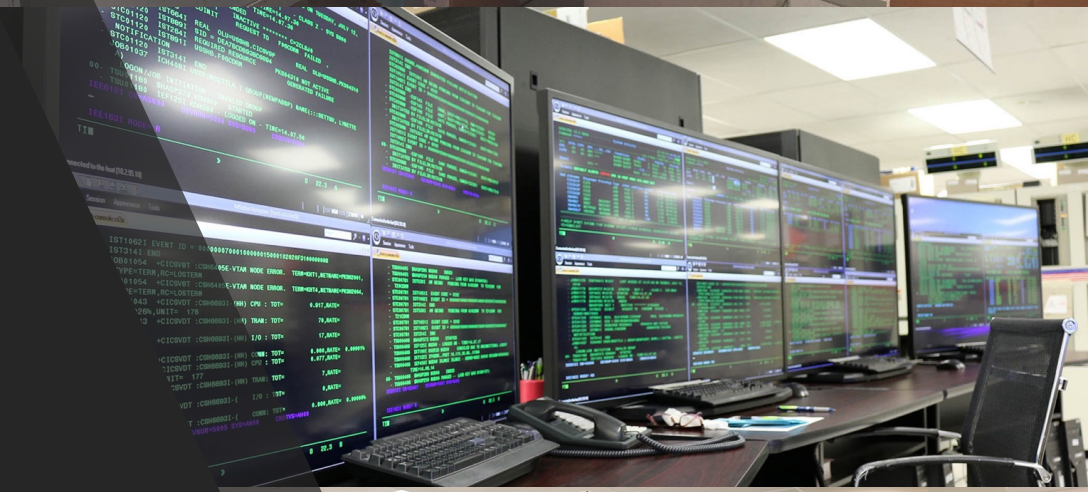
ETS
OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

- Led by Chief Information Officer (CIO)
- Advances programs and projects with the greatest potential to **increase efficiency, reduce waste, and improve transparency and accountability** in State of Hawai‘i government.
- Provides efficient, effective and available IT enterprise services and support in the areas of data center, cybersecurity, computing (mainframe and open systems), telecommunications, application development, and web-based services for the purpose of assisting State government agencies in fulfilling their current and future business mission and objectives.

Where we started

- Decentralized IT (18 different State of Hawaii departments)
- Unreliable IT infrastructure
- Inconsistent policies and standards
- Financial, tax, payroll and other systems and associated processes — all over 40 years old
- Printing more than 42,000 pieces of paper per day
- Nine different email systems for state employees (including Lotus Notes)
- Difficult for 18,000 employees to communicate effectively and efficiently
- Aging IT workforce





Where we are today

IT Governance and new authority to oversee IT projects	NGN (stable, redundant, high-speed) Including public safety radio communications	Enterprise Cybersecurity Enhancements	GIS and Geospatial Program Delivery Enhancements
Colocation Agreement with UH Data Center (resilient backup)	Tax System Modernization (2015-2019)	Enterprise Payroll Modernization (2016-2018)	Paperless Reporting from Mainframe (2018)
Microsoft Office 365	eSign Services	Civil Service IT Broadbanding	Hawaii Annual Code Challenge

State employee-led IT security program

- 2016 Legislature's approval of **new cybersecurity positions,** including a Chief Information Security Officer (CISO) helps further build the State's cybersecurity program

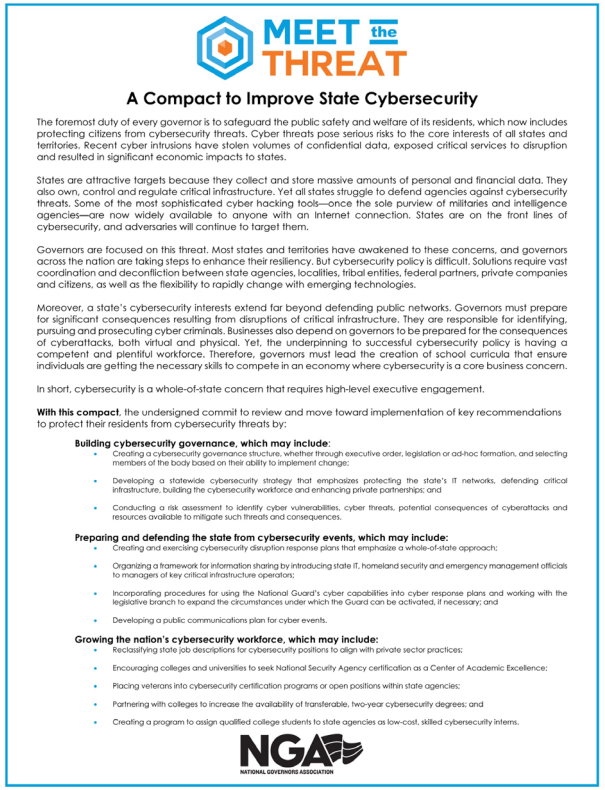
- Positions filled:
  - CISO
  - Support positions
  - Additional recruitment ongoing

- Protects all branches of government that today share a common access point to the Internet — where most cyber threats originate!
- Enables the State to shift a majority of security work previously done by contractors to skilled State personnel.
- Allows ETS to pursue cost-effective solutions for cybersecurity by providing additional training to State employees.

Hawaii joins NGA Cyber Compact

- Multi-state cybersecurity compact signed by 38 governors
- Commitments:
  1. Build cybersecurity governance
  2. Prepare and defend from cybersecurity events
  3. Grow cybersecurity workforce

NATIONAL GOVERNORS ASSOCIATION



MEET the THREAT

A Compact to Improve State Cybersecurity

The foremost duty of every governor is to safeguard the public safety and welfare of its residents, which now includes protecting citizens from cybersecurity threats. Cyber threats pose serious risks to the core interests of all states and territories. Recent cyber intrusions have stolen volumes of confidential data, exposed critical services to disruption and resulted in significant economic impacts to states.

States are attractive targets because they collect and store massive amounts of personal and financial data. They also own, control and regulate critical infrastructure. Yet all states struggle to defend agencies against cybersecurity threats. Some of the most sophisticated cyber hacking tools—once the sole purview of militaries and intelligence agencies—are now widely available to anyone with an Internet connection. States are on the front lines of cybersecurity, and adversaries will continue to target them.

Governors are focused on this threat. Most states and territories have awakened to these concerns, and governors across the nation are taking steps to enhance their resiliency. But cybersecurity policy is difficult. Solutions require vast coordination and deconfliction between state agencies, localities, tribal entities, federal partners, private companies and citizens, as well as the flexibility to rapidly change with emerging technologies.

Moreover, a state's cybersecurity interests extend far beyond defending public networks. Governors must prepare for significant consequences resulting from disruptions of critical infrastructure. They are responsible for identifying, pursuing and prosecuting cyber criminals. Businesses also depend on governors to be prepared for the consequences of cyberattacks, both virtual and physical. Yet, the underpinning to successful cybersecurity policy is having a competent and plentiful workforce. Therefore, governors must lead the creation of school curricula that ensure individuals are getting the necessary skills to compete in an economy where cybersecurity is a core business concern.

In short, cybersecurity is a whole-of-state concern that requires high-level executive engagement.

With this compact, the undersigned commit to review and move toward implementation of key recommendations to protect their residents from cybersecurity threats by:

Building cybersecurity governance, which may include:

- Creating a cybersecurity governance structure, whether through executive order, legislation or ad-hoc formation, and selecting members of the body based on their ability to implement change;
- Developing a statewide cybersecurity strategy that emphasizes protecting the state's IT networks, defending critical infrastructure, building the cybersecurity workforce and enhancing private partnerships; and
- Conducting a risk assessment to identify cyber vulnerabilities, cyber threats, potential consequences of cyberattacks and resources available to mitigate such threats and consequences.

Preparing and defending the state from cybersecurity events, which may include:

- Creating and exercising cybersecurity disruption response plans that emphasize a whole-of-state approach;
- Organizing a framework for information sharing by introducing state IT, homeland security and emergency management officials to managers of key critical infrastructure operators;
- Incorporating procedures for using the National Guard's cyber capabilities into cyber response plans and working with the legislative branch to expand the circumstances under which the Guard can be activated, if necessary; and
- Developing a public communications plan for cyber events.

Growing the nation's cybersecurity workforce, which may include:

- Reclassifying state job descriptions for cybersecurity positions to align with private sector practices;
- Encouraging colleges and universities to seek National Security Agency certification as a Center of Academic Excellence;
- Placing veterans into cybersecurity certification programs or open positions within state agencies;
- Partnering with colleges to increase the availability of transferable, two-year cybersecurity degrees; and
- Creating a program to assign qualified college students to state agencies as low-cost, skilled cybersecurity interns.

NGA
NATIONAL GOVERNORS ASSOCIATION

Cybersecurity trends

- Most breaches occur because basics are not getting done
- Standardizing on platforms, vendor supported
- IT workforce needs
- Privileged access management, no account has admin access 24/7

HONOLULU Star-Advertiser

March 9, 2017 | 73° | Check Traffic

Hawaii News

As many as 45 million cyber attacks hit state networks daily, officials say

By Kevin Dayton
January 12, 2017

BRYANT FUKUTOMI / BFUKUTOMI@STARADVERTISER.COM

Most attacks are launched through malware that may be downloaded from corrupted websites, or can enter systems through thumb drives or other infected equipment, an official said.

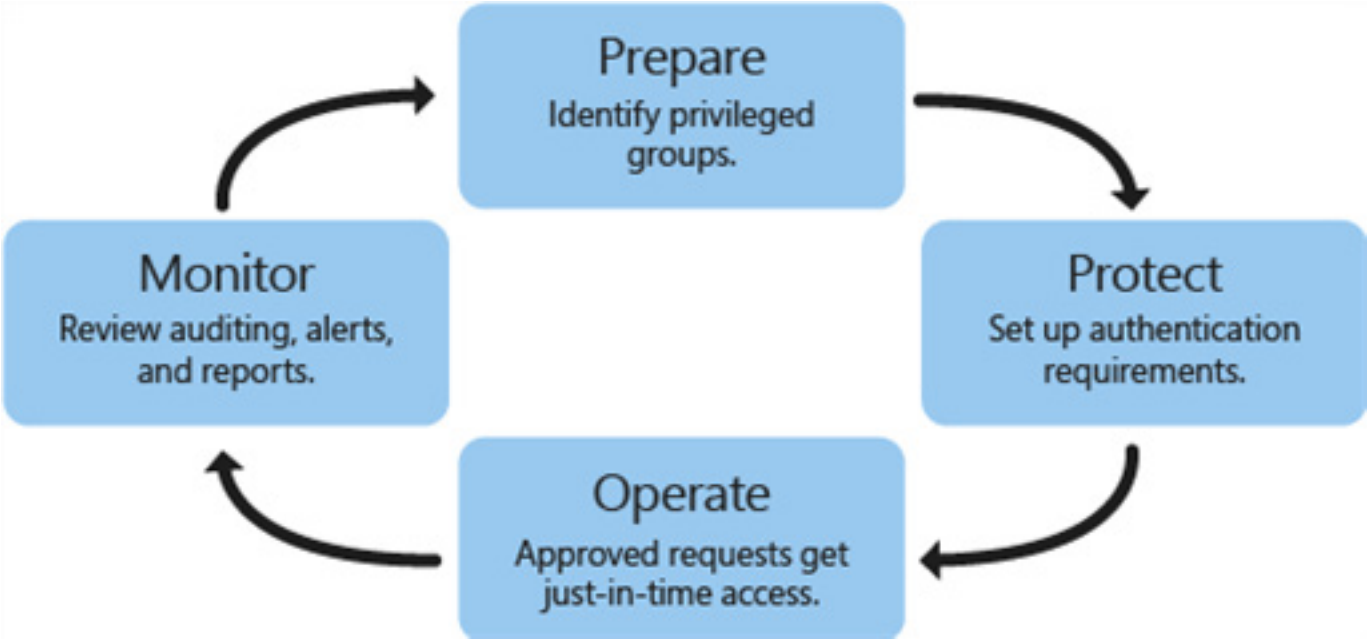
What ETS is doing

- Hired CISO
- Updating security policies
- Penetration testing
- Phishing exercise
- IT governance structure
- IT workforce development

Privileged Access Management (PAM)

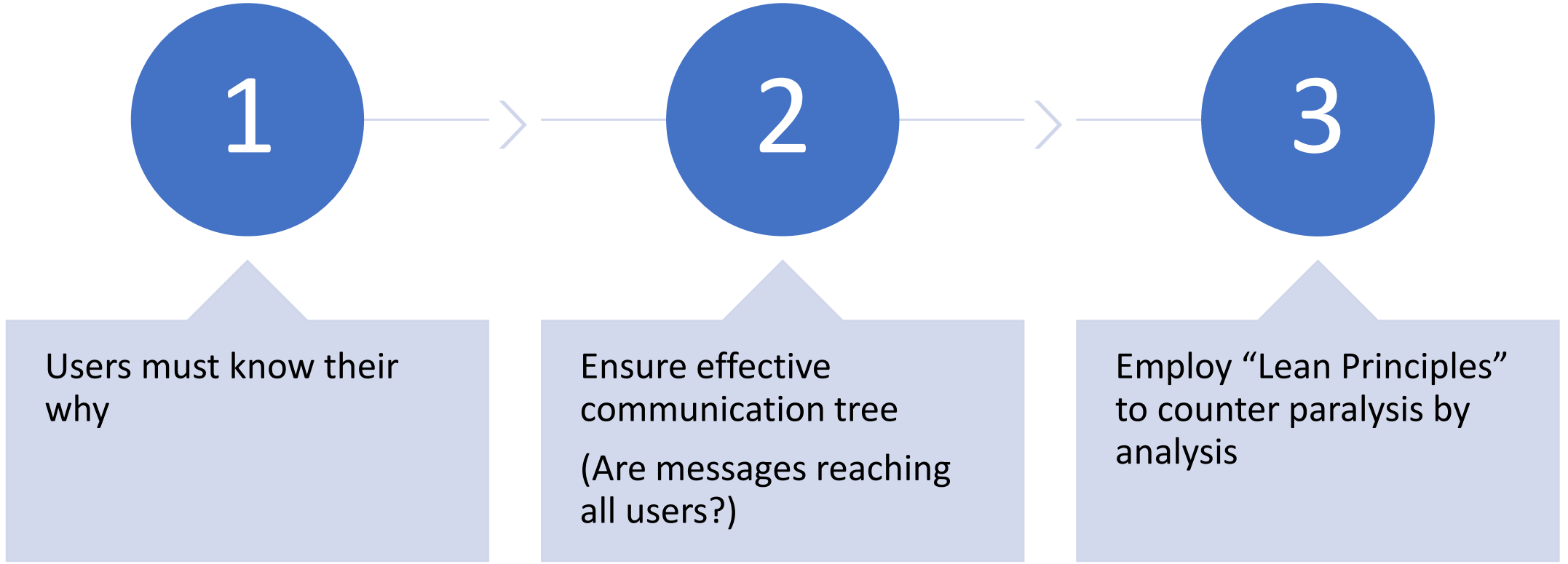
- PAM is a solution that helps organizations restrict privileged access within an existing Active Directory environment.

- Two goals:
  1. Re-establish control over a compromised Active Directory environment by maintaining a separate bastion environment that is known to be unaffected by malicious attacks.
  2. Isolate the use of privileged accounts to reduce the risk of those credentials being stolen.



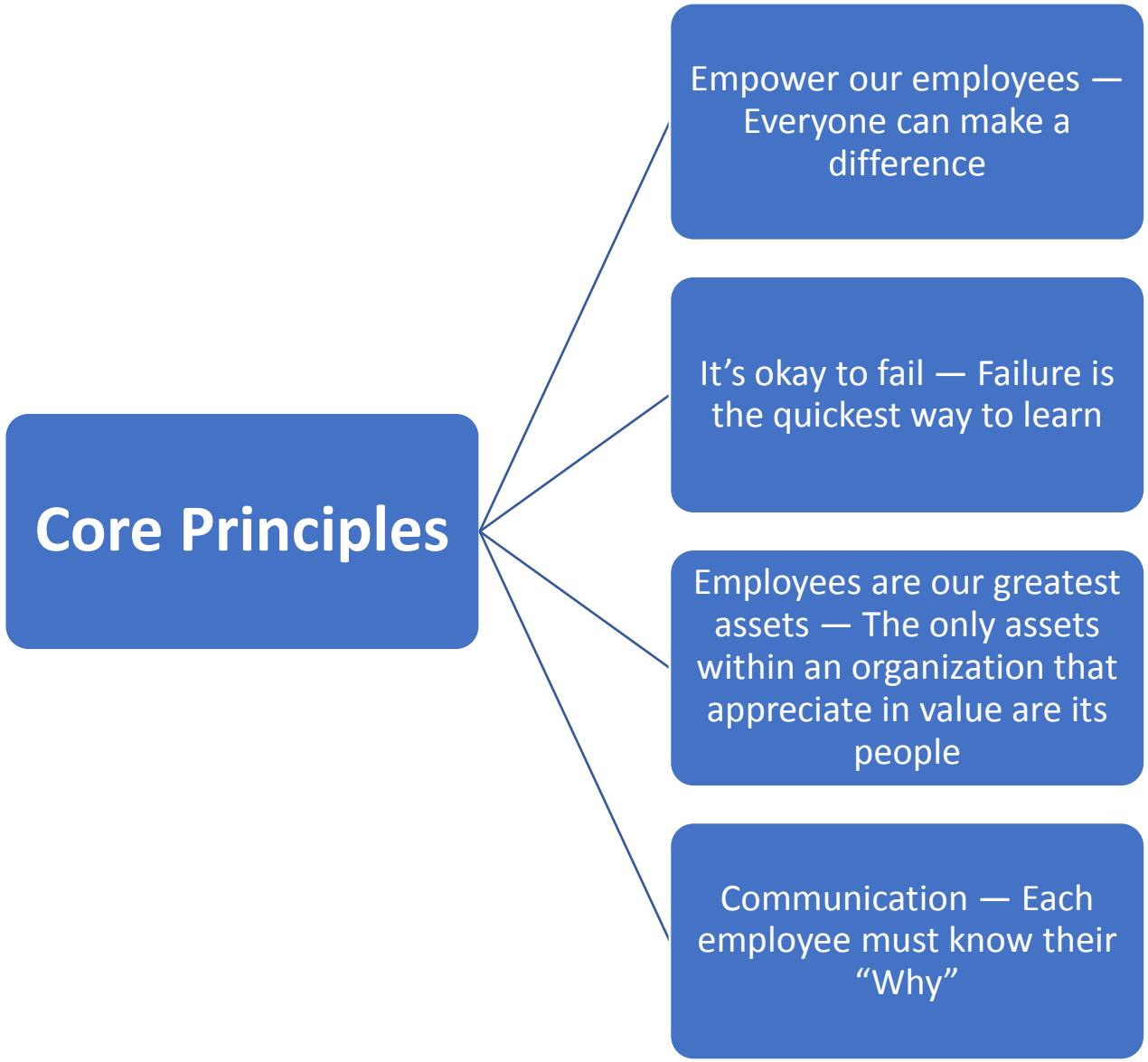
https://docs.microsoft.com/en-us/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

Organizational Change Management (OCM)



How we transformed state government

Our mission: We believe improving the quality of life for the citizens of Hawaii



STATE OF HAWAII 1959
UA·MAU·KE·EA·O·KA·AINA·I·KA·PONO

ETS
OFFICE OF ENTERPRISE TECHNOLOGY SERVICES

Mahalo

EMAIL: ets@hawaii.gov | WEB: ets.hawaii.gov